RTU RĒZEKNE

RTU RĒZEKNES AKADĒMIJA
Inženierzinātņu centrs

REZEKNE ACADEMY OF RIGA TECHNICAL UNIVERSITY
Engineering Centre

VIDE.TEHNOLOĢIJA. RESURSI

XVI starptautiskās zinātniski praktiskās konferences rakstu krājums
2025. gada 19.–20. jūnijs

5. SĒJUMS

ENVIRONMENT. TECHNOLOGY. RESOURCES

Proceedings of the 16th International Scientific and Practical Conference
June 19th – 20th, 2025

VOLUME V



Rēzekne 2025

RTU RĒZEKNES AKADĒMIJA
Inženierzinātņu centrs

REZEKNE ACADEMY
OF RIGA TECHNICAL UNIVERSITY
Engineering Centre

VIDE. TEHNOLOĢIJA. RESURSI

XVI starptautiskās zinātniski praktiskās konferences materiāli
2025.gada 19.-20.jūnijs

5. SĒJUMS

ENVIRONMENT. TECHNOLOGY. RESOURCES

Proceedings of the 16th International Scientific and Practical Conference
June 19th – 20th, 2025

Volume V

Rezekne
2025

VIDE. TEHNOLOĢIJA. RESURSI. 16. starptautiskās zinātniski praktiskās konferences materiāli. 2025.gada 19.-20. jūnijs. 5.*sējums*: RTU Rēzeknes akadēmija, Rēzekne, Latvija, 2025. 370 lpp.

ENVIRONMENT. TECHNOLOGY. RESOURCES. Proceedings of the 16th International Scientific and Practical Conference on June 19-20, 2025. *Volume V*: Rezekne Academy of Riga Technical University, Rezekne, Latvia, 2025. pp. 370.

16.starptautiskās zinātniski praktiskās konferences "Vide. Tehnoloģija. Resursi" materiālos četros sējumos ir pārstāvēti jaunākie pētījumi vides inženierzinātnē, vides un dabas aizsardzībā, ilgtspējīgā lauksaimniecībā, enerģētikā, materiālzinātnē, mehānikā, metālapstrādē, lāzeru tehnoloģijās, matemātiskajā modelēšanā, elektrotehnikā, vides ekonomikā un vadībā, informācijas tehnoloģijās un sociotehnisko sistēmu modelēšanā, vides izglītībā un ilgtspējīgas attīstības procesos, izglītība inženierzinātnēs, aizsardzības un drošības tehnoloģijās. Krājumā pārstāvēto pētījumu joma ir daudzpusīga un starpdisciplināra, balstīta uz starptautisko zinātnieku kolektīvu sasniegumu rezultātiem. Konferences materiālos iekļauti 317 zinātniskie raksti. Konferences dalībnieki pārstāv 28 valstis.

16.starptautiskās zinātniski praktiskās konferences "Vide. Tehnoloģija. Resursi" norises vieta ir RTU Rēzeknes akadēmija, Rēzekne, Latvija.

Proceedings of the 16th International Scientific and Practical Conference "Environment. Technology. Resources" include recent research in fields of engineering, environmental and nature protection, sustainable agriculture, energy, material science, mechanics, metalworking, laser technologies, mathematical modelling, electrical engineering, environmental economics and management, information technologies and sociotechnical systems modelling, environmental education and sustainable development, education in engineering sciences, defense and security technologies. The research area presented in the proceedings is comprehensive and cross-disciplinary, on the advances of international researchers. The proceedings comprise 317 scientific papers. Conference participants represent 28 countries.

16th International Scientific and Practical Conference "Environment. Technology. Resources." hosted by Rezekne Academy of Riga Technical University, Rezekne, Latvia

https://conferences.rta.lv/index.php/ETR/ETR2025
Link to conference proceedings: http://journals.rta.lv/index.php/ETR

This journal is licensed under
Creative Commons Attribution 4.0 International (CC BY 4.0) License
The author(s) of the paper take responsibility for the content of the paper

Online **ISSN 2256-070X**

Published by **RTU PRESS, 2025**

Scientific Committee Chairman

Dr.sc.ing. Edmunds Teirumnieks, Rezekne Academy of Riga Technical University, Latvia

Scientific Committee Co-Chairmen

Dr. Walter Leal, Hamburg University of Applied Sciences, Germany, Manchester Metropolitan University, United Kingdom
Dr.sc.ing. Andris Martinovs, Rezekne Academy of Riga Technical University, Latvia
Dr.sc.ing. Artis Teilāns, Rezekne Academy of Riga Technical University, Latvia

Scientific Committee

Dr.agr. Aleksandrs Adamovičs, Latvia University of Life Sciences and Technologies, Latvia
PhD Nikolaj Angelov, Technical University of Gabrovo, Bulgaria
PhD Kiril Anguelov, Technical University of Sofia, Bulgaria
PhD Andres Annuk, Estonian University of Life Sciences, Estonia
Dr. agr. Lidiia Antypova, Mykolaiv National Agrarian University, Ukraine
PhD Iluta Arbidane, Rezekne Academy of Riga Technical University, Latvia
PhD Plamen Atanasov, New Bulgarian University, Bulgaria
PhD Todor Balabanov, University of Transport "Todor Kableshkov", Bulgaria
PhD Stefan Bankov, The Ministry of Interior of Bulgaria, Bulgaria
PhD Jānis Bičevskis, University of Latvia, Latvia
PhD Aija Brakovska, Daugavpils University, Latvia
PhD Ģirts Būmanis, Riga Technical University, Latvia
PhD Ivan Byanov, University of Veliko Tarnovo "St. Cyril and St. Methodius", Bulgaria
PhD Hamid Can, Trakya University, Turkey
Dr. hab. Ing. Tadeusz Chrzan, Poltegor Institute, Poland
PhD Dimitar Dimitrov, Todor Kableshkov University of Transport, Bulgaria
PhD Sevdalina Dimitrova, “Vasil Levski” National Military University, Bulgaria
PhD Nadezhda Dimova, New Bulgarian University Department "Economics", Bulgaria
PhD Nikolay Dolchinkov, "Vasil Levski" National Military University, Bulgaria
Dr.hist. Edvins Evarts, Turiba University, Latvia
PhD Vanko Ganev, "Vasil Levski" National Military University, Bulgaria
Dr.sc.ing. Imants Gorbāns, Riga Technical University, Latvia
Dr.sc.ing. Aleksandrs Gorbunovs, Riga Technical University, Latvia
Dr.sc.ing. Pēteris Grabusts, Rezekne Academy of Riga Technical University, Latvia
PhD Grigor Grigorov, “Vasil Levski” National Military University, Bulgaria
PhD Inga Grinfelde, Latvia University of Life Sciences and Technologies, Latvia
PhD Tzvetelin Gueorguiev, Technical University of Gabrovo, Bulgaria
PhD Mart Hovi, Estonian University of Life Sciences, Estonia
PhD Maria Ilcheva, Saint Cyril and Methodius University of Veliko Tarnovo, Bulgaria
Dr. agr. Sofija Jankauskiene, Lithuanian Research Centre for Agriculture and Forestry, Lithuania
PhD Aivars Jermuss, Latvia University of Life Sciences and Technologies, Latvia
Dr.sc.ing. Aivars Kaķītis, Latvia University of Life Sciences and Technologies, Latvia
PhD Sabrina Kalinkova, University of National and World Economy, Bulgaria
Dr.paed. Ilmārs Kangro, Rezekne Academy of Riga Technical University, Latvia
PhD Atis Kapenieks, Riga Technical University, Latvia
Dr. paed. Janis Kapenieks, Riga Technical University, Latvia
PhD Tsanko Karadzhov, Technical University of Gabrovo, Bulgaria
PhD Aivars Kaupuzs, Rezekne Academy of Riga Technical University, Latvia
PhD Stancho Kajkov, “Vasil Levski” National Military University, Bulgaria
PhD Anna Khilya, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Spain
PhD Georgi Komitov, Agricultural University Plovdiv, Bulgaria
PhD Inga Ļašenko, Riga Technical University, Latvia
Dr.sc.ing. Lyubomir Lazov, Rezekne Academy of Riga Technical University, Latvia
PhD Iveta Linina, Turiba University, Latvia

PhD Lyuboslav Lyubenov, University of Ruse "Angel Kanchev", Bulgaria
Dr.sc.math. Maksims Marinaki, University of Latvia, Latvia
PhD Rumen Marinov, “Vasil Levski” National Military University, Bulgaria
PhD Dilyan Markov, Georgi Rakovski Military Academy, Bulgaria
Dr.sc.ing. Linda Mežule, Riga Technical University, Latvia
PhD Ziedonis Miklašēvičs, Rezekne Academy of Riga Technical University, Latvia
PhD Nikolai Minkovski, University of Forestry, Bulgaria
PhD Penko Mitev, Technical University of Sofia, Bulgaria
Dr.sc.ing. Ivan Mitev, Technical University of Gabrovo, Bulgaria
PhD Marufjon Musaev, Tashkent State Technical University, Uzbekistan
PhD Nikolay Padarev, "Vasil Levski" National Military University, Bulgaria
Dr.sc.ing. Desislava Petrova, Technical University of Gabrovo, Bulgaria
Dr.agr. Liena Poiša, Rezekne Academy of Riga Technical University, Latvia
Dr. agr. Valentīna Pole, IK Tava zeme, Latvia
PhD Dimcho Pulov, Technical University of Gabrovo, Bulgaria
PhD Aurelija Pūraitė, Mykolas Romeris University, Lithuania
Dr. agr. Gundega Putniece, Latvia University of Life Sciences and Technologies, Latvia
PhD Todor Rachovski, Plovdiv University “Paisii Hilendarski”, Bulgaria
Dr.sc.ing. Ādolfs Ruciņš, Latvia University of Life Sciences and Technologies, Latvia
PhD Rashmi Jaymin-Sanchaniya, Riga Technical University, Latvia
PhD Iryna Sarancha, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Ukraine
PhD Dafinka Sidova, New Bulgaria University, Bulgaria
PhD Inese Skapste, Latvia University of Life Sciences and Technologies, Latvia
Dr.sc.ing. Andris Skromulis, Rezekne Academy of Riga Technical University, Latvia
PhD Krasimir Slavyanov, "Vasil Levski" National Military University, Bulgaria
PhD Nikolay Stefanov, “Vasil Levski” National Military University, Bulgaria
PhD Julija Steinhart, BA School of Banking and Finance, Switzerland
PhD Agrita Švarta, Latvia University of Life Sciences and Technologies, Latvia
PhD Adiljan Suleymanov, Tashkent State Technical University, Uzbekistan
Dr.sc.ing. Artis Teilāns, Rezekne Academy of Riga Technical University, Latvia
Dr.-Ing. Josef Timmerberg, Jade University of Applied Sciences, Germany
Dr.sc.ing. Edmunds Teirumnieks, Rezekne Academy of Riga Technical University, Latvia
PhD Ērika Teirumnieka, Rezekne Academy of Riga Technical University, Latvia
Dr.biol. Rasma Tretjakova, Rezekne Academy of Riga Technical University, Latvia
PhD Dragomir Vassilev, Technical University of Gabrovo, Bulgaria
PhD Valentin Vassilev, South-West University "Neofit Rilski", Bulgaria
PhD Tsanka Zlateva-Petkova, Technical University of Gabrovo, Bulgaria
PhD Anda Zvaigzne, Rezekne Academy of Riga Technical University, Latvia
PhD Rosita Zvirgzdina, Turiba University, Latvia

Organising Committee Chairman

PhD Nikolay Dolchinkov, "Vasil Levski" National Military University, Bulgaria

Organising Committee

Dr.agr. Aleksandrs Adamovičs, Latvia University of Life Sciences and Technologies, Latvia
Dr. agr. Lidiia Antypova, Mykolaiv National Agrarian University, Ukraine
MA Yanitsa Boyanova, “Vasil Levski” National Military University, Bulgaria
Dr.sc.ing. Aleksandrs Gorbunovs, Riga Technical University, Latvia
Dr.sc.ing. Pēteris Grabusts, Rezekne Academy of Riga Technical University, Latvia
Dr.sc.ing. Ēriks Kronbergs, Latvia University of Life Sciences and Technologies, Latvia
Dr.sc.ing. Sergejs Kodors, Rezekne Academy of Riga Technical University, Latvia
Dr. paed. Janis Kapenieks, Riga Technical University, Latvia
PhD Tsanko Karadzhov, Technical University of Gabrovo, Bulgaria
Dr.sc.ing. Lyubomir Lazov, Rezekne Academy of Riga Technical University, Latvia
Dr.sc.ing. Andris Martinovs, Rezekne Academy of Riga Technical University, Latvia

PhD Rumen Marinov, “Vasil Levski” National Military University, Bulgaria
Dr.agr. Liena Poiša, Rezekne Academy of Riga Technical University, Latvia
Dr.sc.ing. Andris Skromulis, Rezekne Academy of Riga Technical University, Latvia
Dr.-Ing. Josef Timmerberg, Jade University of Applied Sciences, Germany
Dr.sc.ing. Artis Teilāns, Rezekne Academy of Riga Technical University, Latvia
Mg.sc.comp. Gundega Teilāne, Rezekne Academy of Riga Technical University, Latvia
PhD Ērika Teirumnieka, Rezekne Academy of Riga Technical University, Latvia

Reviewers

PhD Nikolaj Angelov, Technical University of Gabrovo, Bulgaria
PhD Andres Annuk, Estonian University of Life Sciences, Estonia
PhD Neli Arabadzhieva - Kalcheva, Technical University of Varna, Bulgaria
PhD Iluta Arbidane, Rezekne Academy of Riga Technical University, Latvia
PhD Svetlana Asmuss, University of Latvia, Latvia
PhD Plamen Atanasov, New Bulgarian University, Bulgaria
Dr.sc.ing. Anita Avišāne, Riga Technical University, Latvia
PhD Todor Balabanov, University of Transport "Todor Kableshkov", Bulgaria
PhD Yanka Baneva, Medical University Varna, Bulgaria
Dr.agr. Biruta Bankina, Latvia University of Life Sciences and Technologies, Latvia
PhD Stefan Bankov, The Ministry of Interior of Bulgaria, Bulgaria
PhD Sholpan Bekmukhanbetova, Kazakh Automobile and Road Institute, Kazakhstan
PhD Daniel Berchev, “Vasil Levski” National Military University, Bulgaria
PhD Ansis Ataols Bērziņš, Riga Technical University, Latvia
PhD Jānis Bičevskis, University of Latvia, Latvia
PhD Aija Brakovska, Daugavpils University, Latvia
Dr. Rene Brunsch, Apromace data systems GmbH, Germany
PhD Ģirts Būmanis, Riga Technical University, Latvia
PhD Ivan Byanov, University of Veliko Tarnovo "St. Cyril and St. Methodius", Bulgaria
PhD Basar Caglar, Izmir Institute of Technology, Turkey
Dr.hab.Ing. Tadeusz Chrzan, Poltegor Institute, Poland
PhD Maria Chunchukova, Agricultural University Plovdiv, Bulgaria
PhD Dimitar Dimitrov, "Georgi Benkovski", Bulgarian Air Force Academy, Bulgaria
PhD Dimitar Dimitrov, Todor Kableshkov University of Transport, Bulgaria
PhD Sevdalina Dimitrova, “Vasil Levski” National Military University, Bulgaria
PhD Nadezhda Dimova, New Bulgarian University Department "Economics", Bulgaria
PhD Nikolay Dolchinkov, "Vasil Levski" National Military University, Bulgaria
Dr.hist. Edvins Evarts, Turiba University, Latvia
Dr. agr. Daina Feldmane, Institute of Horticulture, Latvia
PhD Vanko Ganev, "Vasil Levski" National Military University, Bulgaria
PhD Dmitri Goljandin, Tallinn University of Technology, Estonia
Dr.sc.ing. Imants Gorbāns, Riga Technical University, Latvia
PhD Jānis Grabis, Riga Technical University, Latvia
PhD Grigor Grigorov, “Vasil Levski” National Military University, Bulgaria
PhD Inga Grinfelde, Latvia University of Life Sciences and Technologies, Latvia
Dr. agr. Elvyra Gruzdevienė, Flax museum, the branch of Eriskiai Cultural Center of the Panevezys District, Lithuania
PhD Ilze Gudro, Riga Technical University, Latvia
PhD Tzvetelin Gueorguiev, Technical University of Gabrovo, Bulgaria
PhD Mart Hovi, Estonian University of Life Sciences, Estonia
PhD Maria Ilcheva, Saint Cyril and Methodius University of Veliko Tarnovo, Bulgaria
PhD Valery Ivanov, Defense Institute "Professor Tsvetan Lazarov", Bulgaria
Dr. agr. Sofija Jankauskiene, Lithuanian Research Centre for Agriculture and Forestry, Lithuania
PhD Aivars Jermuss, Latvia University of Life Sciences and Technologies, Latvia
PhD Amit Joshi, BA School of Banking and Finance, Latvia
Dr.sc.ing. Aivars Kaķītis, Latvia University of Life Sciences and Technologies, Latvia
PhD Sabrina Kalinkova, University of National and World Economy, Bulgaria

Dr.paed. Ilmārs Kangro, Rezekne Academy of Riga Technical University, Latvia
PhD Veiko Karu, Estonian Business School, Estonia
PhD Aivars Kaupuzs, Rezekne Academy of Riga Technical University, Latvia
PhD Anna Khilya, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Spain
PhD Andrejs Koliškins, Riga Technical University, Latvia
PhD Georgi Komitov, Agricultural University Plovdiv, Bulgaria
PhD Karīne Laganovska, Latvian University of Biosciences and Technologies, Malnava College, Latvia
PhD Vjaceslavs Lapkovskis, Riga Technical University, Latvia
PhD Inga Ļašenko, Riga Technical University, Latvia
PhD Lazar Lazarov, "Vasil Levski" National Military University, Bulgaria
Dr. Walter Leal, Hamburg University of Applied Sciences, Germany, Manchester Metropolitan University, United Kingdom
Dr.sc.ing. Angel Lengerov, Technical University of Plovdiv, Bulgaria
PhD Iveta Linina, Turiba University, Latvia
Dr.oec. Jelena Lonska, Rezekne Academy of Riga Technical University, Latvia
PhD Slobodan Lubura, University of East Sarajevo, Bosnia and Herzegovina
PhD Lyuboslav Lyubenov, University of Ruse "Angel Kanchev", Bulgaria
PhD Velichko Machev, Todor Kableshkov University of Transport, Bulgaria
Dr.sc.math. Maksims Marinaki, University of Latvia, Latvia
PhD Georgi Marinov, Rakovski National Defence College, Bulgaria
PhD Dilyan Markov, Rakovski National Defence College, Bulgaria
PhD Arturs Medveckis, Liepaja Academy of Riga Technical University, Latvia
Dr.sc.ing. Linda Mežule, Riga Technical University, Latvia
PhD Ziedonis Miklašēvičs, Rezekne Academy of Riga Technical University, Latvia
PhD Roussi Minev, Ruse University, Bulgaria
PhD Nikolai Minkovski, University of Forestry, Bulgaria
PhD Penko Mitev, Technical University of Sofia, Bulgaria
Dr.sc.ing. Ivan Mitev, Technical University of Gabrovo, Bulgaria
PhD Ilie Nuca, Technical University of Moldova, Republic of Moldova
Dr.chem. Sergejs Osipovs, Daugavpils University, Latvia
PhD Nikolay Padarev, "Vasil Levski" National Military University, Bulgaria
PhD Jana Paidere, Daugavpils University, Latvia
Dr.sc.ing. Jeļena Pečerska, Riga Technical University, Latvia
Dr.sc.ing. Desislava Petrova, Technical University of Gabrovo, Bulgaria
PhD Valentina Petrova, Nikola Vaptsarov Naval Academy, Bulgaria
Dr. agr. Valentīna Pole, IK Tava zeme, Latvia
PhD Dimcho Pulov, Technical University of Gabrovo, Bulgaria
PhD Aurelija Pūraitė, Mykolas Romeris University, Lithuania
Dr. agr. Gundega Putniece, Latvia University of Life Sciences and Technologies, Latvia
PhD Todor Rachovski, Plovdiv University "Paisii Hilendarski", Bulgaria
PhD Anton Rassolkin, Tallinn University of Technology, Estonia
Dr.phys. Gita Rēvalde, Riga Technical University, Latvia
Dr.sc.ing. Ādolfs Ruciņš, Latvia University of Life Sciences and Technologies, Latvia
PhD Jolanta Šadauskiene, Kaunas University of Technology, Lithuania
Dr.sc.math. Felikss Sadirbajevs, Daugavpils University, Latvia
PhD Rashmi Jaymin-Sanchaniya, Riga Technical University, Latvia
PhD Iryna Sarancha, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Ukraine
PhD Zhaneta Savova, National Military University, Bulgaria
Dr.geol. Valdis Segliņš, University of Latvia, Latvia
PhD Dafinka Sidova, New Bulgaria University, Bulgaria
PhD Andrejs Šiškins, Riga Technical University, Latvia
PhD Inese Skapste, Latvia University of Life Sciences and Technologies, Latvia
PhD Krasimir Slavyanov, "Vasil Levski" National Military University, Bulgaria
Dr.-Ing. Bambang Soemardiono, Institut Teknologi Sepuluh Nopember, Indonesia
Dr.geol. Juris Soms, Daugavpils University, Latvia
PhD Nikolay Stefanov, "Vasil Levski" National Military University, Bulgaria

PhD Julija Steinhart, BA School of Banking and Finance, Switzerland
PhD Aina Strode, Rezekne Academy of Riga Technical University, Latvia
PhD Agrita Švarta, Latvia University of Life Sciences and Technologies, Latvia
Dr.sc.ing. Edmunds Teirumnieks, Rezekne Academy of Riga Technical University, Latvia
PhD Plamen Teodosiev, University of Library Studies and Information Technologies, Bulgaria
Dr.biol. Rasma Tretjakova, Rezekne Academy of Riga Technical University, Latvia
PhD Dragomir Vassilev, Technical University of Gabrovo, Bulgaria
PhD Valentin Vassilev, South-West University "Neofit Rilski", Bulgaria
Dr.habil.sc.ing. Janis Viba, Riga Technical University, Latvia
PhD Emil Yankov, Rezekne Academy of Riga Technical University, Latvia
Dr.sc.ing. Imants Zarembo, Rezekne Academy of Riga Technical University, Latvia
PhD Tsanka Zlateva-Petkova, Technical University of Gabrovo, Bulgaria
PhD Anda Zvaigzne, Rezekne Academy of Riga Technical University, Latvia
PhD Rosita Zvirgzdina, Turiba University, Latvia

Secretariat Chairman

PhD Ērika Teirumnieka, Rezekne Academy of Riga Technical University, Latvia

Secretariat Members

Dr.agr. Liena Poiša, Rezekne Academy of Riga Technical University, Latvia
Mg.sc.comp. Gundega Teilāne, Rezekne Academy of Riga Technical University, Latvia

V SĒJUMS
SATURS
CONTENTS

Defence and Security Technologies

Andrii Andres, Olha Rymar, Nataliia Sorokolit, Hanna Huk, Valerii Kryzhanovskyi **15**
OPTIMIZATION OF CADETS' PSYCHOPHYSICAL FITNESS THROUGH INDIVIDUAL TRAINING PROGRAMS

Petar Arabadzhiyski, Valentin Vasilev, Dafinka Sidova **23**
EFFECTIVE HUMAN RESOURCE MANAGEMENT AND ENVIRONMENTAL SECURITY: PROTECTION OF HUMAN ENVIRONMENTAL RIGHTS AND CRITICAL INFRASTRUCTURE SUSTAINABILITY

Plamen Atanasov **29**
ANALYSIS OF THE COLD WAR FOR PUBLIC OPINION, AND THE INTERESTS IN THE CYBERSPACE

Daniela Atanasova, Nadezhda Krasteva **37**
ENVIRONMENTAL PROTECTION AND THE NEW SAFEGUARDS PROVIDED IN DIRECTIVE (EU) 2024/1203 ON THE PROTECTION OF THE ENVIRONMENT THROUGH CRIMINAL LAW

Vasil Andonov, Yordan Shterev **43**
IDENTIFYING AND ANALYZING DJI DRONE SIGNALS

Ilona Bulgakova, Artūrs Gaveika, Ilga Krampuža **51**
DIGITAL TECHNOLOGICAL AND LEGAL SUPPORT OF THE ILLEGAL MIGRATION CONTROL: A POPULATION AND NATIONAL SECURITY ASPECTS

Gabriela Belova, Gergana Georgieva, Yosif Kochev, Aleksandar Yankov, Vladimir Babanov **57**
COVID-19, INFODEMIC AND CYBER SECURITY

Daniel Berchev, Milko Stefanov **63**
DESIGN OF THE TRAINING – APPROACH FOR IDENTIFICATION OF THE REQUIREMENTS TO THE EDUCATIONAL PROCESS IN THE MILITARY EDUCATION SYSTEM

Jordan Deliversky **69**
THE ROLE OF DIGITALIZATION IN THE FIGHT AGAINST CORRUPTION

Todor Dimitrov **73**
LEGAL ASPECTS OF EUROPEAN UNION ARMAMENTS COOPERATION: CHALLENGES AND OPPORTUNIES FOR INTEGRATION

Nikolay Todorov Dolchinkov, Nikolay Iliyanov Padarev **81**
RADIOACTIVE WASTE STORAGE AS AN ELEMENT OF NATIONAL SECURITY

Nikolay Todorov Dolchinkov, Nikolay Bonev Nichev **89**

USING DRONES TO CLEAN CONTINENTAL WATER BODIES

Grigor Grigorov, Svilen Spirdonov **97**
ANALYSIS OF THE POSSIBILITIES FOR VISUALIZING THE RISK OF DISASTERS AND ACCIDENTS IN THE AREAS OF CRITICAL INFRASTRUCTURE SITES THROUGH GIS APPLICATIONS

Genadiy Gospodinov, Lyubomir Gotsev, Tamara Ristovska, Svetlana Syarova, Viktoriya Angelova **103**
CYBERSECURITY IN SMART CITIES: A REVIEW OF THEORETICAL MODELS, EMERGING THREATS, AND DEFENCE STRATEGIES

Teodora Georgieva, Ivo Radulov **111**
MODERN VIEWS IN THE ANALYSIS AND EVALUATION OF COMMAND AND CONTROL SYSTEMS

Mirosław Grewiński, Marek Kawa **119**
THE ROLE OF INSECTS AND WORMS AS AGENTS OF BIOTERRORISM IN THE ATMOSPHERE OF POST- 9/11 AMERICA

Ivan Ivanov, Sevdalin Spassov **127**
ELECTRONIC ATTACK USING SDR

Krasimir Koynakov **135**
RESEARCH OF THE ENERGY STATUS OF MILITARY PERSONNEL DURING COMPLEX TACTICAL EXERCISES

Inga Kudeikina, Sandra Kaija, Ivans Jānis Mihailovs, Lidija Juļa, Vitālijs Rakstiņš **141**
SECURITY IN LEGAL EDUCATION: CHALLENGES AND SOLUTIONS IN THE MODERN WORLD

Andrii Kalabskyi, Serhii Romanchuk, Nataliia Sorokolit, Artur Oderov, Orest Loiko **149**
MODERN INNOVATIVE APPROACHES OF DOMESTIC AND FOREIGN EXPERTS TO MODERNIZE THE PHYSICAL TRAINING OF FEMALE SERVICEWOMEN

Lyuboslav Lyubenov **155**
CRIMINAL LAW EDUCATION AS A COMPONENT OF THE NATIONAL SECURITY SYSTEM OF THE REPUBLIC OF BULGARIA

Rumen Marinov **163**
THE DYNAMICS OF MILITARY SECURITY – CHALLENGES AND FORECASTS IN THE CONDITIONS OF GLOBAL (IN)SECURITY

Rumen Marinov **171**
COLLECTIVE DEFENSE – A MEANS TO ACHIEVE A MORE SUSTAINABLE FUTURE

Dilyan Markov **179**
A CHANGE IN THE WAY ARTILLERY IS USED, BASED ON THE RUSSIA-UKRAINE CONFLICT

Dilyan Markov **185**
INFLUENCE OF ARMED CONFLICTS ON METHODS FOR DETERMINING FIRING DATA FOR HITTING ARTILLERY TARGETS

Boyan Mitrakiev, Noncho Dimitrov **191**

TRACING REFLEXIVE CONTROL APPLICATION IN THE ANTI-SHALE GAS MOVEMENTS IN EASTERN EUROPE

Svilen Neykov **201**
EXAMINING THE IMPACT OF IMAGE AUGMENTATION ON OBJECT DETECTION AND CLASSIFICATION TO IMPROVE PERFORMANCE OF SITUATIONAL AWARENESS SYSTEMS

Nikolay Nichev, Krasimir Koynakov **209**
A MODEL FOR USING DRONES FOR MEDICAL RECONNAISSANCE IN COMBAT OPERATIONS

Nikolay Iliyanov Padarev, Nikolay Dolchinkov **213**
ANALYSIS OF A RADIOLOGICAL INCIDENT IN NUCLEAR POWER PLANT AND SIMULATION OF THE RADIOACTIVE MATERIAL DISPERSION

Nikolay Iliyanov Padarev **219**
ADJUSTING THE QUANTITY OF SURFACTANTS IN DECONTAMINATION SOLUTIONS

Aurelija Pūraitė, Danguolė Seniutienė **225**
MIGRATION AS A HYBRID THREAT: LEGAL PERSPECTIVES ON COUNTERING ILLEGAL MIGRATION AND THE LITHUANIA-BELARUS BORDER CRISIS

Ivo G. Radulov **237**
METHODS FOR DESCRIPTION, ANALYSIS AND EVALUATION OF COMMAND AND CONTROL SYSTEMS (C2)

Raphael Röttinger **247**
IMPLEMENTING THE CAPABILITIES OF THE ATLAS NETWORK TO IMPROVE THE EUROPEAN UNION'S COUNTER-TERRORISM EFFORTS

Miroslav Stefanov, Boyan Jekov, Tito Titov, Andriyan Stoilov, Kiril Nikolov **255**
EXPLORING THE POTENTIAL OF ARTIFICIAL INTELLIGENCE TO PREDICT CYBER ATTACKS: CREATION, EVALUATION AND COMPARATIVE ANALYSIS OF EFFECTIVE MODELS OF FINE-TUNING, RANDOM FORESTS, AND NEURAL NETWORKS

Vladislavs Sardiko, Dzintra Ilisko **265**
THE IMPACT OF CHANGE MANAGEMENT ON THE QUALITY OF THE WORK ENVIRONMENT: A STUDY OF THE EMPLOYER-EMPLOYEE RELATIONSHIP OF SENIOR CUSTOMS SUPERVISORS

Sandra Škutāne, Krišjānis Kuplis, Ilze Avotiņa **271**
SPEED TESTS AND CONTROL EXERCISES IN SPORTS PRACTICE

Milko Stefanov, Daniel Berchev **277**
INTEGRATION PROCESSES IN THE MILITARY EDUCATION SYSTEM

Nikolay Penchev Stefanov
GLOBALIZATION AND GLOBAL SECURITY **285**

Dimitrina Stefanova, Kristiana Bacheva, Valentin Vasilev **291**

CONCEPTUAL CONVERGENCE: DISINFORMATION, FAKE NEWS, AND INFORMATION INFLUENCE AS A TRIAD OF SECURITY THREATS IN THE CONTEXT OF SOCIETY 5.0

Veselka Stoyanova **297**
PREREQUISITES FOR THE ESTABLISHMENT OF A QUANTUM STEGANOGRAPHY COMMUNICATION

Dace Šulmane **303**
DEFENSE CONCEPT THROUGH THE LEGISLATURE – PROTECTING VALUES FOR THE SUSTAINABILITY OF SOCIETY

Plamen Teodosiev, Pavlina Nikolova **311**
RESEARCH ON ARTIFICIAL INTELLIGENCE PLATFORMS WITH THE POSSIBILITY OF APPLICATION IN DIPLOMATIC ACTIVITIES

Laila Vaivode **317**
JOINT INFORMATION SYSTEM MODEL APPLIANCE IN MAN-MADE CRISIS MANAGEMENT

Gergana Varbanova **323**
APPLICATION OF DEEP LEARNING IN ARTIFICIAL INTELLIGENCE SYSTEMS FOR CYBERATTACK IDENTIFICATION AND PREVENTION

Violeta Vasiliauskienė, Anželika Banevičienė, Vykintas Stumbrys **329**
BUSINESS ACTIONS POSING THREAT TO NATIONAL SECURITY

Svetoslav Yordanov **341**
SWARMING TERRORIST ATTACK AS AN EVOLVING THREAT FOR THE EUROPEAN SECURITY

Zarko Zdravkov, Anelia Atipova **349**
METHODOLOGY FOR ASSESSMENT OF A NATIONAL SECURITY SYSTEM

Martin Zahariev, George Dimitrov, Daniela Pavlova, Panayot Gindev, Vyara Savova, Radoslava Makshutova **353**
KEY TAKEAWAYS FROM THE MOST SIGNIFICANT GDPR PERSONAL DATA BREACHES IN THE REPUBLIC OF BULGARIA

Zhuliyan Zhelezov **363**
IMPLICATIONS OF INTERNATIONAL LAWFARE FOR THE GLOBAL SECURITY ARCHITECTURE

V
DEFENCE AND SECURITY TECHNOLOGIES

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 15-21

Optimization of Cadets' Psychophysical Fitness Through Individual Training Programs

Andrii Andres
Associate Professor of the Department of Physical Education
Lviv Polytechnic National University
Lviv, Ukraine
andres-a@ukr.net

Olha Rymar
Associate Professor of the Department of Theory and Methods of Physical Education
Ivan Boberskyi Lviv State University of Physical Culture
Lviv, Ukraine
okopiy@ukr.net

Nataliia Sorokolit
Professor of the Department of Theory and Methods of Physical Culture
Ivan Boberskyi Lviv State University of Physical Culture
Lviv, Ukraine
sorokolit21@gmail.com

Hanna Huk
Lecturer at the Department of Theory and Methods of Physical Education
Ivan Boberskyi Lviv State University of Physical Culture
Lviv, Ukraine
annahook14@gmail.com

Valerii Kryzhanovskyi
Graduate student Department of Theory and Methods of Physical Education
Ivan Boberskyi Lviv State University of Physical Culture
Lviv, Ukraine
krizanovskiyv77@gmail.com

***Abstract* - The necessity of individualizing military training for cadets and servicemen is driven by technological advancements and changes in combat tactics. The specialized literature emphasizes the importance and timeliness of an individualized approach; however, the methods of its implementation are not specified. Purpose. The study aims to identify groups of cadets with similar professionally important qualities, develop their characteristics, and justify approaches to individualizing the process of physical training and sports to enhance the effectiveness of military-professional activities. Methodology. A survey was conducted among cadets (n=282) of the Kyiv Institute of the National Guard of Ukraine. The questionnaire included standard methodologies for assessing anxiety levels (STAI), emotional control (Cortlaud Emotional Control Scale), life satisfaction (SWLS, Diener, Emmons, Larsen, and Griffith), and coping strategies (R. Lazarus and S. Folkman). The physical fitness levels of cadets (n=282) were also tested. Descriptive statistics and cluster analysis methods were applied. Results. The cadets were divided into clusters based on their physical fitness and psycho-emotional characteristics. Five groups with relatively homogeneous indicators were identified. We developed "profiles" of psychophysical preparedness. The use of these profiles allowed us to substantiate approaches to individualizing the physical training and sports processes for cadets of five different types to ensure effective military-professional training. During physical training, appropriate physical loads were selected for cadets in each group, considering volume and intensity. Recommendations were provided on suitable physical activities for independent training for cadets of different types. Conclusions. The implementation of an individualized approach to cadets' physical training, particularly through group segmentation, improves their professionally important qualities, enhances physical fitness, and increases competencies in physical education and sports, ultimately contributing to the effectiveness of their military-professional activities.**

Keywords: physical fitness, anxiety, emotional control, life satisfaction, coping strategies.

I. INTRODUCTION

In the current context of military aggression on the territory of Ukraine, there is an urgent need to improve the psychophysical readiness of military personnel. This necessity is driven by the insufficient preparedness of security and defense sector personnel to operate effectively under extreme and psychologically challenging conditions [1; 2; 3]. Psychophysical readiness plays a crucial role in ensuring the long-term effectiveness of professional activity in stressful environments [4; 5]. Physical training and sports are foundational to the professional development of future specialists [6; 7], as

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8487
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

there is a proven link between physical fitness and psycho-emotional stability [8; 9]. Recent research also highlights the importance of individualizing military training for cadets and service members [10–13]. However, the lack of consistent and systematic data in the specialized literature complicates the development of effective training programs for cadets of higher educational institutions of the National Guard of Ukraine. This undermines their ability to perform professional duties efficiently, resist burnout, and ultimately weakens national defense and public safety.The aim of the study is to identify groups of cadets with similar professionally significant qualities, develop their characteristics, and justify approaches to the individualization of physical training and sports to improve the effectiveness of their military-professional activities.

II. MATERIALS AND METHODS

A survey was conducted among cadets (n=282) of the Kyiv Institute of the National Guard of Ukraine. The questionnaire included standardized methods to determine the level of anxiety (STAI), emotional control (Cortlaud Emotional Control Scale), life satisfaction (SWLS, Diener, Emmons, Larsen, and Griffith), and coping strategies (R. Lazarus and S. Folkman). The level of physical fitness of cadets (n=282) was also tested.

TABLE 1 PHYSICAL FITNESS INDICATORS OF CADET CLUSTERS

Indicators	**Clusters**	**M**	**SD**	**SE**	**Score points**	**Median**	**Variance**	**Shapiro-Wilk**	
								W	***p***
3000 m run, sec	1	741,65	43.38	9.0466	5	750.00	1882.328	0.941	0.187
	2	782.64	70.28	13.2834	3	780.00	4940.534	0.967	0.496
	3	773.44	33.32	4.1991	3	780.00	1110.832	0.909	< .001
	4	751.11	32.92	3.8275	4-5	750.00	1084.098	0.964	0.033
	5	767.83	38.22	7.8030	3-4	765.00	1461.275	0.898	0.020
Shuttle run 10×10 m, sec	1	54.22	7.61	1.5867	2	53.00	57.905	0.949	0.283
	2	28.54	5.90	1.1156	4	27.00	34.851	0.842	< .001
	3	31.86	5.96	0.7450	2	29.00	35.520	0.874	< .001
	4	30.43	5.37	0.6247	2	28.00	28.879	0.851	< .001
	5	55.50	7.54	1.5405	2	54.00	56.957	0.936	0.134
Pull-over exercise, reps	1	7.65	3.47	0.7240	5	6.00	12.055	0.850	0.003
	2	10.75	7.91	1.4957	5	10.00	62.639	0.910	0.020
	3	6.14	3.80	0.4750	5	5.00	14.440	0.811	< .001
	4	8.57	5.03	0.5855	5	6.00	25.372	0.751	< .001
	5	5.25	2.27	0.4633	4	4.50	5.152	0.832	0.001
Pull-ups on a horizontal bar, reps	1	16.17	4.07	0.8497	5	15.00	16.605	0.927	0.096
	2	16.96	6.05	1.1449	5	17.50	36.702	0.975	0.726
	3	12.81	3.06	0.3831	3	13.00	9.393	0.974	0.202
	4	15.49	4.35	0.5063	5	15.00	18.966	0.953	0.008
	5	12.67	2.03	0.4156	3	13.00	4.145	0.951	0.278
Grenade throwing, m	1	40.78	6.09	1.2698	5	38.00	37.087	0.881	0.011
	2	35.68	12.50	2.3632	4	35.00	156.374	0.937	0.093
	3	34.17	6.45	0.8069	4	34.50	41.668	0.936	0.003
	4	38.09	8.78	1.0209	5	36.00	77.128	0.745	< .001
	5	34.17	6.09	1.2448	4	34.00	37.188	0.968	0.608
Complex strength exercise, reps	1	56.61	9.14	1.9077	5	55.00	83.704	0.795	< .001
	2	50.57	12.90	2.4389	4	52.00	166.550	0.894	0.008
	3	48.84	5.28	0.6600	4	48.50	27.880	0.940	0.004
	4	51.97	5.80	0.6743	5	52.00	33.643	0.930	< .001
	5	48.58	3.61	0.7370	4	49.50	13.036	0.885	0.011
Pistol shooting, hits	1	2.83	0.38	0.0808	4	3.00	0.150	0.463	< .001
	2	2.82	0.39	0.0737	4	3.00	0.152	0.468	< .001
	3	2.59	0.52	0.0658	4	3.00	0.277	0.660	< .001
	4	2.74	0.47	0.0546	4	3.00	0.221	0.558	< .001
	5	2.79	0.41	0.0847	4	3.00	0.172	0.503	< .001
Obstacle course, sec	1	101.74	8.75	1.8245	4-5	102.00	76.565	0.964	0.543
	2	163.39	11.80	2.2309	2	162.00	139.358	0.934	0.080
	3	126.97	6.37	0.7974	3	129.00	40.697	0.943	0.005
	4	103.14	7.65	0.8904	4	104.00	58.666	0.909	< .001
	5	122.17	8.95	1.8274	3	121.00	80.145	0.957	0.386

To quantitatively describe the empirical data, the method of descriptive statistics was applied. Cluster analysis was performed to identify groups of cadets with similar characteristics, needs, or behaviors and to segment them into groups. This segmentation allows for a better understanding of the target audience of cadets and facilitates the development of more effective training strategies for them.

III. RESULTS AND DISCUSSION

Physical Readiness. The analysis of indicators (Table 1) showed that a normal distribution was mostly not

observed. The summarized data confirmed that all cadet clusters demonstrated a high level of physical qualities. The only test in which cadets performed poorly was the shuttle run (10×10 m), as indicated by low scores in four clusters.

Based on the generalization of the results of our study, we were able to distinguish five clusters of cadets with relatively homogeneous psycho-emotional indicators and physical fitness levels. The cluster analysis provided comprehensive information about the performance levels and their assessments for representatives of each cluster.

Cadets in the first cluster were characterized by relatively high physical fitness levels. They exhibited well-developed endurance, strength endurance, and specialized endurance. However, their performance in the shuttle run 10×10 m (54.22±7.61 s) indicated a low level of specialized (speed) endurance.

The second cluster demonstrated the highest performance in the pull-over exercise (10.75±7.91 reps) and pull-ups on a horizontal bar (16.96±6.05 reps), which received the highest scores. This suggests a relatively superior level of upper body strength and strength endurance.

The third cluster had average results in almost all test exercises. They showed a relatively low level of specialized endurance but a high level of upper body strength endurance. The fourth cluster stood out with the highest overall physical fitness level. Their performance in grenade throwing (38.09±8.78 m) indicated the highest level of speed strength. The only weak point was the shuttle run, which received a low score (2 points), although their result (30.43±5.37 s) was not the worst among the clusters.

In contrast, the fifth cluster had the lowest level of physical fitness. The results of five test exercises were significantly lower than those of the other clusters.

Psycho-emotional indicators (Table 2). The life satisfaction scores (23.61±6.68 points) characterized participants of the first two clusters as somewhat satisfied with life. In contrast, in the third cluster, this score (20.68±7.54 points) was closest to the average level (20 points). The fifth cluster was conditionally named the "average group" since none of its indicators were rated as extreme (either maximum or minimum) compared to other clusters. The second and third clusters contained the most and least satisfied cadets, respectively.

TABLE 2 PSYCHO-EMOTIONAL INDICATORS OF CADET CLUSTERS

Indicators	General data		Cluster 1		Cluster 2		Cluster 3		Cluster 4		Cluster 5	
	Mean	*SE*	*Mean*	*SD*	*Mean*	*SD*	*Mean*	*SD*	*Mean*	*SD*	*Mean*	*SD*
Life Satisfaction	22.28	0.4438	22.63	7.85	23.61	6.68	20.68	7.54	21.61	8.84	22.70	7.18
State Anxiety	57.10	0.6145	59.42	10.83	58.00	10.41	56.25	9.59	54.87	9.50	57.87	10.27
Trait Anxiety	58.84	0.6354	60.08	10.75	59.58	10.57	57.21	12.27	57.43	8.31	59.11	10.99
Aggression Control	15.66	0.2709	15.92	4.59	16.45	3.98	15.50	4.89	15.04	4.38	16.11	4.32
Depression Control	14.35	0.2924	13.67	4.45	14.95	4.60	14.07	5.62	13.70	5.09	14.47	4.82
Anxiety Control	13.61	0.2423	13.67	3.56	14.31	3.24	14.11	5.61	13.74	3.80	14.13	3.97
Confrontational Coping	7.03	0.2302	6.54	3.45	6.89	3.52	7.71	4.46	6.04	3.78	7.02	3.74
Distancing	6.52	0.2291	5.79	3.01	7.00	3.32	7.32	4.55	6.09	3.82	6.83	3.61
Self-Control	8.56	0.2717	8.13	3.95	9.02	4.44	9.21	5.51	7.83	4.51	8.88	4.60
Seeking Support	7.39	0.2327	6.58	3.26	7.78	3.55	8.36	5.04	6.30	3.97	7.67	3.92
Acceptance of Responsibility	4.61	0.1639	4.50	2.47	4.86	2.38	4.82	3.33	4.26	3.05	4.78	2.63
Escape-Avoidance	7.95	0.2796	7.46	3.81	7.88	4.36	9.39	5.88	6.96	3.84	8.16	4.69
Problem-Solving Planning	9.38	0.2889	8.83	4.68	9.77	4.81	9.54	5.19	8.26	4.50	9.52	4.85
Positive Reappraisal	8.98	0.2784	7.71	3.56	9.13	4.50	10.57	5.32	7.48	4.47	9.18	4.60

The highest anxiety scores, both state anxiety (59.42±10.83 points) and trait anxiety (60.08±10.75 points), were observed among cadets in the first cluster. Meanwhile, cadets in the fourth cluster had relatively lower anxiety levels (54.87±9.50 points and 57.43±8.31 points, respectively).

The level of emotional control was moderate across all clusters. However, the control (suppression) of anxiety and depression in cadets of the first cluster was relatively the lowest (13.67±4.45 points and 13.67±3.56 points, respectively). The highest indicators of emotional control were observed in the second cluster, indicating a relatively high level of suppression (aggression – 16.45±3.98 points, depression – 14.95±4.60 points, anxiety – 14.31±3.24 points). The anger levels of cadets in the fourth cluster were relatively the lowest (15.04±0.914 points).

Confrontational coping was the lowest in cadets of the fourth cluster and was rated below the general data level

(6.04±4.38 points), indicating a low level. Similar low values were recorded in the first cluster (6.54±3.45 points). The highest indicators of confrontational coping were found in cadets of the third cluster (7.71±4.46 points).

A similar situation was observed in distancing: the lowest indicator was recorded in cadets of the first cluster, rated below the general data level (5.79±3.01 points), which is considered a low level. Low values were also noted in the fourth cluster (6.09±3.82 points), while the highest values were recorded in the third cluster (7.32±4.55 points).

In the coping strategy of seeking support, the trend was similar: it was the lowest in cadets of the fourth cluster and was rated below the general data level (6.30±3.97 points), indicating a low level. Low values were also observed in the first cluster (6.58±3.26 points). The highest values were found in the third cluster (8.36±5.04 points).

Self-control showed a similar pattern, except that cadets in the first cluster had moderate rather than low indicators (8.13±3.95 points). However, cadets of the third cluster had the highest values (9.21±5.51 points), consistent with previous subscales. Cadets of the fourth cluster had the lowest values relative to other clusters (7.83±4.51 points), but these were rated as moderate rather than low, unlike the previous subscales.

For the escape-avoidance subscale, cadets of the third cluster had slightly higher indicators (9.39±5.58 points) than in previous subscales. The lowest values were found in cadets of the fourth cluster (6.96±3.84 points), which were considered low.

Regarding positive reappraisal, cadets of the third cluster had the highest indicators (10.57±5.32 points) compared to previous subscales, rated as a moderate level. Cadets of the fourth cluster had the lowest indicators relative to other clusters (7.48±4.47 points), also rated as a moderate level.

For the acceptance of responsibility subscale, all clusters were rated at a low level. However, the lowest values were in the fourth cluster (4.26±3.05 points), while the highest were not in the third but in the second cluster (4.86±0.297 points).

The same trend was observed for the problem-solving planning coping strategy: the lowest indicators were found in the fourth cluster (8.26±4.50 points), while the highest were in the second cluster (9.77±4.81 points). The only difference was that these indicators were rated as moderate.

Thus, five "profiles" of cadets' psychophysical readiness were developed, grouping individuals with similar professionally important qualities. Summarizing the results of this study and the data from specialized literature allowed us to substantiate approaches to individualizing physical training and sports for cadets of five types to ensure successful preparation for military-professional activities.

TABLE 3 RECOMMENDED MEANS OF PHYSICAL ACTIVITY FOR CADETS OF DIFFERENT TYPES OF PSYCHOPHYSICAL READINESS

Means of Physical Training and Sports	**Types**				
	A	*B*	*C*	*D*	*E*
Team sports	*		*	*	*
Aerobic exercises: CrossFit, sports orienteering, tennis, swimming, etc.		*	*		
Beep test, shuttle run 10×10 m	*		*	*	*
Military-applied exercises, sports, and multiathlon			*	*	*
Martial arts, combat sports (sambo, combat horting, hand-to-hand combat)	*	*	*		*
Tasks that highlight leadership roles (group leader)	*		*	*	*
Shooting, accuracy exercises, highly coordinated sports			*	*	*
Mountaineering, sport climbing	*		*		*
Horseback riding, yoga, meditation	*	*			*
Military-applied obstacle courses					

The application of the developed "profiles" of cadets' psychophysical readiness during physical training will allow for the selection of appropriate physical loads for cadets from each group (Table 3).

Cadets of Type A are recommended to focus on the enhanced development of specific (speed) endurance while maintaining a balanced development of other physical qualities to sustain the achieved level. They should use physical training and sports activities that reduce anxiety and enhance stress resilience. Team sports, particularly handball, can be beneficial for this purpose [14]. To prevent intense emotional reactions to frustration, it is advisable to develop distancing and confrontation coping strategies. Although confrontation is often perceived as maladaptive, moderate use ensures resistance to difficulties, energy, and initiative in problem-solving, as well as the ability to stand up for oneself and cope with anxiety in stressful conditions [15; 16; 17]. Cadets of this cluster should also be encouraged to apply techniques for developing responsibility skills and to engage in providing support to others.

Cadets of Type B are advised to undergo conditioning training to maintain their level of physical fitness. Special attention should be given to developing aerobic endurance, specific endurance, and agility. Activities such as cross-country running, orienteering, rowing, and cardio workouts are recommended. Exercises involving obstacle courses, military-sports pentathlon, and complex coordination sports (martial arts) can also be beneficial. Additionally, they should be involved in training other cadets to develop responsibility skills.

Cadets of Type C should prioritize physical training, particularly developing muscular endurance in the arms and torso. Their training should include motor activities that foster the ability to defend their interests and cope

with anxiety in stressful situations (confrontational coping strategies).

Cadets of Type D should engage in conditioning training to maintain their level of physical development across all fitness components.

Cadets of Type E are recommended to engage in intensive physical training to improve their overall physical fitness. To enhance their weakest physical attributes, they should incorporate additional activities such as team sports, complex coordination sports (martial arts), and military pentathlon. These activities aim to improve their shuttle run (10x10 m) and pull-up performance. Additional exercises on a single obstacle course or military-sports pentathlon training are also recommended.

The physical readiness of military personnel is closely linked to their psychological resilience. Studies confirm that physical training is a critical factor for stress resistance and combat effectiveness [11; 12; 18; 19; 20]. Research findings [12] emphasize that physical conditioning directly impacts a soldier's ability to function under stress, contributing to overall success in military operations. Physical preparedness is crucial for soldiers to meet the evolving demands of modern warfare. Coordination skills are considered key components of physical fitness, influencing psychophysical readiness for operations in extreme conditions [20]. In this context, specialized training programs that combine high-intensity workouts with firearms and tactical training are seen as promising [11]. The advantage of such programs lies in their systematic approach, incorporating physical assessments, intensive development of fitness qualities, specialized training, and a maintenance phase to retain results. Essential success factors in military training include moral qualities [18] and personal characteristics [19].

Modern research underscores the necessity of individualizing military training for cadets and personnel due to technological advancements and changes in combat tactics [10]. At the same time, limited access to sports facilities during wartime highlights the importance of alternative approaches to physical self-improvement, particularly individual physical training within military academies [21]. Studies indicate that senior cadets are primarily motivated by personal goals in physical training. Therefore, military training programs should be highly differentiated. Based on the psychophysical readiness model for future officers, integrating physical and psychological training is essential for improving performance and reducing anxiety in various combat scenarios [22]. Research findings [18; 19; 20; 21; 22] highlight the significance of both physical and psychological qualities in military personnel across different service branches, emphasizing their role in combat readiness and mission success. This necessitates a comprehensive approach, including not only physical and theoretical training but also the development of moral, psychological, and professionally essential qualities.

An individualized approach to military training enhances learning efficiency and combat readiness. Studies [23; 24] show that implementing personalized training programs in military units is beneficial and yields better results compared to traditional group training methods. In the Ukrainian context [25], the importance of an individualized approach for each cadet is emphasized, fostering creative thinking and independent work. Proposed measures for improving officer and non-commissioned officer training systems aim to equip cadets with new educational and professional competencies, ensuring interoperability with NATO forces. Alongside curriculum modifications, a revised methodology for training sessions has been introduced, focusing on creative problem-solving and individualized instruction. However, while specialized literature highlights the importance of individualized training, specific implementation methods are often lacking. The inconsistent and fragmented data available make it challenging to develop structured individualized training programs for cadets.

To design individualized training programs aimed at developing the professionally essential qualities of cadets, we have identified five types of psychophysical readiness based on characteristic indicators.

Type A is characterized by the lowest levels of specific endurance and speed-strength but the highest levels of aerobic and muscular endurance. These cadets exhibit strong emotional reactions to stressful situations (including war), low stress resilience, and poor control over depression and anxiety. They are typically passive and struggle to defend their interests.

Type B demonstrates high performance across all physical tests, particularly in pull-ups and leg raises. However, they perform poorly in obstacle course runs. These cadets are the most satisfied with life, highly stress-resilient, and have a strong sense of responsibility in problem-solving.

Type C has an average level of physical fitness, with relatively weak results in comprehensive strength exercises. They exhibit the lowest levels of personal anxiety but report the lowest life satisfaction. These cadets tend to use aggressive coping strategies, struggle with planning and foresight, and actively seek support. However, they view difficult situations as opportunities for self-development.

Type D achieves the highest results in most physical tests and has the lowest levels of situational anxiety and aggression. Their coping strategies indicate a lack of ability to actively confront difficulties, an unclear understanding of their personal role in overcoming problems, and a dependent or overly expectant attitude toward others. Nonetheless, they effectively control their emotions and behavior, solve problems systematically, and strive for personal growth.

Type E has the lowest performance in most physical tests, except for pistol shooting and the 3000-meter run, where they maintain average scores. In terms of psychological characteristics, this group demonstrates "average" results, which can be considered an adaptive and optimal level.

Thus, by assessing cadets' physical preparedness, we can propose intervention programs aimed at correcting their "weaker" aspects of psychophysical readiness.

Our proposed classification of cadets into groups facilitates the individualization of physical training and sports activities by:

- ✓ Defining the content focus of training sessions to develop the necessary physical and psycho-emotional qualities for professional duties;
- ✓ Optimally selecting physical workloads for each group;
- ✓ Rationally adjusting training intensity based on cadets' psychophysical readiness type;
- ✓ Encouraging self-directed engagement in individually selected sports activities.

The individualized approach to cadet training, based on psychophysical readiness types, formed the foundation of our technology for developing professionally essential qualities among cadets of the National Guard of Ukraine through physical training and sports [26]. We have demonstrated the high predictive effectiveness of this technology [27]. Its integration into the educational process has contributed to cadets' competencies in individualizing physical training and sports, developing physical qualities, and applying appropriate training techniques. These improvements have led to increased levels of physical fitness. The positive results obtained support the recommendation to implement this technology in the training programs of military education institutions preparing specialists for Ukraine's security and defense sector.

IV. CONCLUSIONS

We identified five types of psychophysical readiness among cadets, each differing in a set of professionally essential qualities.

We developed recommendations for individualizing cadet training based on their psychophysical readiness type.

We established that applying an individualized approach, particularly through classification into groups, fosters the development of professionally essential qualities, enhances physical preparedness, and cultivates competencies in physical training, ultimately improving the effectiveness of military-professional activities.

REFERENCES

[1] V. S. Otkydach, "Improvement of Cadets' Special Physical Training Through Military-Sports All-Around Competitions," dissertation, Prydniprovska State Academy of Physical Culture and Sports, Dnipro, 2023.

[2] Yu. Pavlova, I. Bodnar, V. Kryzhanovskyi, and V. Shvets, "Psychophysical Condition of Cadets—Future Military Law Enforcement Officers in Wartime," in Physical Culture in University Education: Global Practices and Modern Trends, Proc. Int. Sci.-Pract. Conf., Dnipro: Dnipro State Univ. of Internal Affairs, Apr. 13, 2023, pp. 54–57.

[3] V. Pylypchak, "Improving the Physical Training of Cadets in Military Higher Education Institutions Through CrossFit at the Initial Training Stage," dissertation, Lviv State University of Physical Culture named after Ivan Boberskyi, Lviv, 2021.

[4] O. M. Olkhovyi, Theoretical and Methodological Foundations of Professionally-Oriented Physical Training of Cadets in Military Higher Educational Institutions of the Armed Forces of Ukraine, monograph, Kharkiv: KhUPS, 2012.

[5] S. Kostiv, A. Oderov, V. Yagypov, S. Romanchuk, O. Matveiko, V. Baidala, O. Lesko, M. Ostrovsky, O. Kuprinenko, and O. Sydorko, "Experimental results of the psychophysical endurance development of military professionals," Journal of Physical Education and Sport, vol. 21, no. 2, pp. 1076–1083, 2021. DOI: 10.7752/jpes.2021.s2135.

[6] Yu. V. Verenha, "Improvement of Physical Training of Employees of the Ministry of Internal Affairs of Ukraine at the Stage of Professional Development," abstract, Lviv, 2015.

[7] N. Vysochina, L. Hunina, O. Khatsayuk, V. Tomashevskyi, and A. Titovych, "Enhancing the Professional Competencies of Officers—Specialists in Physical Training and Sports in the Use of Modern Interactive Technologies," Military Education, no. 2(42), pp. 76–88, 2020.

[8] N. Caddick and B. Smith, "The impact of sport and physical activity on the well-being of combat veterans: A systematic review," Psychology of Sport and Exercise, vol. 15, no. 1, pp. 9–18, 2013. DOI: 10.1016/j.psychsport.2013.09.011.

[9] Andres, V. Kryzhanovskyj, I. Krasovska, et al., "The influence of agility indicators on formation of vocational readiness in law enforcement officers," in International Scientific Conference «SOCIETY, INTEGRATION, EDUCATION – SIE 2023», vol. I, May 26, 2023, pp. 165–179. Available: http://journals.rta.lv/index.php/SIE/article/view/7105/6068.

[10] O. Kulagin, "Individual Training of Military Personnel in Modern Conditions," in Military Affairs and National Security, 5th ISPC "Scientific Goals and Purposes in XXI Century," Aug. 19-20, 2023, Seattle, USA, no. 36(167), DOI: 10.51582/interconf.19-20.08.2023.034.

[11] K. Kyslenko, "A Complex of High-Intensity Training for Physical, Fire, and Tactical-Special Training of Military Personnel (Specialists in Security Activities)," Scientific Papers of the Interregional Academy of Personnel Management. Pedagogical Sciences, no. 1(60), pp. 26–32, 2024, DOI: 10.32689/maup.ped.2024.1.5.

[12] A.Nedilko, T. Bohun, and V. Dmytryshyna, "Pedagogy of Physical Education in Military Personnel Training: Methods and Approaches to the Development of Physical Activity," Collection of Scientific Papers of the National Academy of the State Border Guard Service of Ukraine, Pedagogical Sciences Series, no. 3(38), pp. 162–182, 2024, DOI: 10.32453/086vvs27.

[13] A.Andres, N. Sorokolit, A. Mandiuk, O. Rymar, and O. Khanikiants, "The impact of sports activities on the psycho-emotional state of cadets in higher education institutions during wartime," ETR, vol. 4, pp. 23–26, Jun. 2024, doi: 10.17770/etr2024vol4.8206.

[14] S. V. Fedorchuk, D. D. Ivaskevych, O. V. Borysova, I. O. Kogut, V. L. Marynych, S. V. Tukaiev, and Y. I. Petrushevskyi, "Application of Coping Strategies in Modern Handball Practice," Sports Medicine, Physical Therapy, and Ergotherapy, vol. 1, pp. 10–15, 2019, DOI: 10.32652/spmed.2019.1.10-15.

[15] P. T. Bartone, "Psychosocial development and leader performance of military officer cadets," Development and Learning in Organizations, vol. 22, no. 2, 2008, doi: 10.1108/dlo.2008.08122bad.009.

[16] O. Fedorenko, V. Dotsenko, I. Okhrimenko, K. Radchenko, and D. Gorbenko, "Coping behavior of criminal police officers at

different stages of professional activity," Broad Research in Artificial Intelligence and Neuroscience, vol. 11, no. 2, pp. 124–146, 2020, doi: 10.18662/brain/11.2/78.
[17] H. Johnsen, J. C. Laberg, and J. Eid, "Coping strategies and mental health problems in a military unit," Military Medicine, vol. 163, no. 9, pp. 599–602, 1998, doi: 10.1093/milmed/163.9.599.
[18] O. Shemchuk, V. Havryushenko, and N. Verbyn, "Scientific and Theoretical Aspects of the Morality Psychology of Military Personnel in the Contemporary Russian-Ukrainian War," Bulletin of the National Defense University of Ukraine, vol. 72, no. 2, pp. 146–160, 2023, DOI: 10.33099/2617-6858-2023-72-2-146-160.
[19] Volkov, "Leading Personal Traits of Military Personnel in Airborne Troops," Journal of Psychology Research, vol. 26, no. 9, pp. 48–60, 2020.
[20] V. O. Lisowski and R. Yu. Mihuta, "Importance of coordination skills essential psycho-physical demonstrated competencies as a military specialists," Physical Education of Students, vol. 6, pp. 38–42, 2013.
[21] A.Chudyk and O. Mozoev, "Individual Physical Training of Cadets in Wartime Conditions," Collection of Scientific Papers of the National Academy of the State Border Guard Service of Ukraine. Pedagogical Sciences Series, vol. 30, no. 3, pp. 565–577, 2022, DOI: 10.32453/pedzbirnyk.v30i3.1180.
[22] N. Vysochyna, L. Hunina, O. Khatsaiuk, L. Kotlyarenko, R. Holovashchenko, and A. Ivchenko, "Model of Psychophysical Readiness of Future Officers to Perform Tasks as Intended," Military Education, vol. 1, no. 43, pp. 24–43, 2021, DOI: 10.33099/2617-1783/2021-43/24-42.
[23] "Impact of a 5-week individualised training program on physical and occupational performance in army recruits," Journal of Science and Medicine in Sport, vol. 25, no. 1, pp. 13–18, 2022.
[24] Outcome-Based Training and Education, Army University Press, n.d.
[25] O. Strutsynskyi, "Current Aspects of Military Specialist Training in Conditions of Hybrid Armed Conflict," Science and Technology of the Air Force of the Armed Forces of Ukraine, vol. 2, no. 43, pp. 38–42, 2021, DOI: 10.30748/NITPS.2021.43.05.
[26] A.S. Andres and V. O. Kryzhanovskyi, "Technology for Developing Professionally Important Qualities of Cadets of Higher Educational Institutions of the National Guard of Ukraine through Sports and Physical Training," Ukrainian Copyright Certificate, no. 121020, Aug. 2, 2023.
[27] A.Andres, I. Bodnar, and V. Kryzhanovskyj, "Effectiveness of the technology for developing professionally important qualities of cadets of higher education institutions of the National Guard of Ukraine through sports and physical training," Health Problems of Civilization, 2024, doi: 10.5114/hpc.2024.139342.

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 23-28

Effective Human Resource Management and Environmental Security: Protection of Human Environmental Rights and Critical Infrastructure Sustainability

Petar Arabadzhiyski
Department of "National and International Security"
New Bulgarian University
Sofia, Bulgaria
parabadzhiyski@gmail.com

Valentin Vasilev
National Security
Higher School of Security and Economics
Plovdiv, Bulgaria
valentin.vasilev@vusi.bg

Dafinka Sidova
Department of "National and International Security"
New Bulgarian University
Sofia, Bulgaria
dsidova@nbu.bg

Abstract- **The scientific paper aims to analyze the interaction between three main areas: the protection of environmental human rights, the resilience of critical infrastructure, and human resource management. These elements are interconnected and play an important role in developing and implementing effective management decisions and policies, combining environmental protection with care for human capital.**

The paper analyses key characteristics of environmental security as a dimension of the Human Security Concept, as well as the role of environmental rights. Additionally, the need to protect critical infrastructure in the context of environmental risks and threats is emphasized.

The focus is placed on new aspects of human resource management, such as green human resources management, the role of so-called "green collars", employee motivation, and others. In this context, the role of effective human resource management in organizations that manage critical infrastructure is examined, to achieve sustainable outcomes in areas related to environmental security.

The third fundamental element of the paper involves practical challenges in implementing the trends and new aspects described above. Ideas and practices are proposed to support the development of solutions for creating sustainable outcomes and policies in human resource management within the context of environmental security.

Keyword- Critical Infrastructure, Environmental Security, Human Resources Management.

I. INTRODUCTION

Analyzing environmental security as a dimension of the Human Security Concept, it is crucial to consider three key areas of activity: the protection of human environmental rights, the resilience of critical infrastructure, and the effective management of human resources. For the purposes of this report, each of these three areas is perceived as a component of a comprehensive model, presented in a basic form but allowing visualization of the continuous interaction between these components. Moreover, the cyclic nature of the interconnectivity and interdependence of these three key areas enables a deeper examination not only of each domain individually but also of the relationships between them, the processes taking place, and the results achieved.

Following this idea, the objective of the study is not only to present key characteristics of the protection of human environmental rights, the resilience of critical infrastructure, and the effective management of human resources but also to identify the correlation between these three components (see Fig. 1).



Fig. 1. Author's Model of Interaction between the three main components of Human Security's Environmental Dimension.

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8484
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

Identifying the common characteristics and scientific relations is presented through an analysis of the interaction between three main areas: the protection of environmental human rights, the resilience of critical infrastructure, and human resource management. These elements are interconnected and play an important role in the development and implementation of effective management decisions and policies, combining environmental protection with human capital care.

Proposing ideas and practices to help find solutions for creating sustainable results and policies in human resource management in the context of environmental security is an attempt to draw the attention of researchers and practitioners to this increasingly significant area in national security management.

With the growing importance of environmental security, there is an urgent need to develop sustainable policies and practices that integrate environmental protection and human resource management. In this context, the protection of environmental rights and the resilience of critical infrastructure are not only legal issues but also strategic concerns that affect national and international security.

II. Materials and Methods

A. Protection of Environmental Human Rights as a component of the Human Security's Environmental Dimension

Environmental security, as a dimension of the Human Security Concept, is directly related to its three pillars: "freedom from fear," "freedom from want," and "freedom for a dignified life" [1], [2]. The definition of "environmental security" focuses primarily on achieving a balance between the physical development and survival of the population benefiting from environmental resources without depleting or diminishing their quality. It aims to ensure a sufficiently favorable environment, equipped with resources in both quantitative and qualitative terms. These resources must be equally accessible to all people and guarantee sustainable development for the global population [3]. It is a set of the status of various systems, such as natural, urbanized, socio-economic, and infrastructural systems (especially those with critical importance). Alongside this, it encompasses the processes that occur between these systems, ensuring that no critical situations or threats arise from environmentally hazardous events, nor do harmful ecological phenomena, impacts, or adverse effects occur on human life, health, and well-being.

According to some authors, environmental security is freedom from fear of environmental harm and ecological threats [4]. The fear of natural catastrophes and disasters caused by anthropogenic, technological, or industrial activities haunts people both personally and professionally. Once provoked, threats of an ecological nature cause not only significant material damage but also loss of human lives in homes and workplaces. In other words, people can lose both their freedom from fear (e.g., in life and health threats) and their freedom from want (e.g., in a deteriorated work environment). In such scenarios, negative processes are triggered that endanger freedom for a dignified life (e.g., forming "environmental nihilism" at the political, managerial, organizational [5], and even societal level).

Another important term related to ensuring the environmental dimension of human security is "environmental human rights." These rights consist in ensuring fair and equal access to essential natural resources (including land, shelter, food, water, and air), which make survival possible both in personal and professional aspects. Three main environmental human rights are distinguished: the right to a safe, clean, healthy, and sustainable environment (including the working environment); the right to clean and accessible drinking water; and the right to safe and accessible sanitary conditions (and working conditions) [6]. These rights must be guaranteed in every aspect of human life—personal, professional, social, and public, etc.

The Updated National Security Strategy of the Republic of Bulgaria clearly emphasizes the connection between environmental security and the sustainability of critical infrastructure. A significant aspect of protecting environmental security (including environmental human rights) involves preventing, controlling, and overcoming the consequences of pollution of soil, water, and air, and the destruction of natural resources due to accidents in strategically important facilities with critical significance for society and the state [7].

At the heart of the Human Security Concept and the Human Resource Management Concept is the individual with their needs, values, character traits, rights, and freedoms. While the Human Security Concept encompasses all aspects of human life, the Human Resource Management Concept focuses on the person in their social role as an employee with professional goals and aspirations for development. It is important to note that in both concepts, guaranteeing environmental human rights is crucial for their high effectiveness.

B. Resilience of Critical Infrastructure as a component of the Human Security's Environmental Dimension

In today's world, critical infrastructure is fundamental to the functioning of society and the economy. It includes networks and systems such as energy, transportation, water supply, communications, and healthcare services, which are vital for the daily lives and safety of citizens. In accordance with the National Climate Change Adaptation Strategy and Action Plan for Infrastructure Resilience 2023, developed by the Ministry of Environment and Water of the Republic of Bulgaria, the resilience of this infrastructure is directly linked to the effective management of human resources and the preparedness of organizations to adapt to new realities arising from environmental risks and climate change [8]. These aspects are particularly important in the context of Bulgaria but are also applicable within the broader European framework.

The resilience of critical infrastructure in the context of effective human resource management (HRM) and

environmental security can be examined through four key aspects. The first one is related to critical infrastructure and its importance in the context of environmental risks. Critical infrastructure must not only be protected from physical and technical threats but also be resilient to challenges arising from climate disasters, natural catastrophes, and other environmental risks. Climate change and the increasing frequency of extreme weather events—such as floods, earthquakes, hurricanes, and high temperatures—necessitate long-term planning and strategic management of infrastructure networks. The ability to adapt to these risks depends not only on technologies but also on the preparedness and training of personnel responsible for managing and operating these systems. This is highlighted in the European Commission's Notice on "Technical Guidance for Climate Resilience of Infrastructure Projects 2021-2027" [9].

The second aspect is the importance of human resources in ensuring resilience. The resilience of critical infrastructure depends on the preparedness of employees to respond effectively in crisis situations. This requires both specialized technical skills and a strategic approach to human resource development. A European Commission press release from October 18, 2022, on accelerating efforts to build European resilience in critical infrastructure, emphasizes that employee training for handling natural disasters and climate change must be integrated into the core of HRM policies.

Regular training, simulations, and emergency response drills will improve reaction times and reduce risks to infrastructure [10]. Developing a culture of resilience is essential, where employees actively participate in adapting to new environmental realities. In this context, HRM strategies should focus on motivating employees to apply principles of resilience and environmental responsibility in their daily work. This includes both motivating the implementation of green practices and developing mechanisms to encourage innovation in infrastructure management.

The third aspect are challenges and approaches to sustainable management of critical infrastructure. One of the biggest challenges for sustainable critical infrastructure management is integrating new technologies that facilitate adaptation to climate change and minimize environmental risks. For example, implementing smart monitoring systems for climate and environmental conditions allows for rapid response and prevention of potential infrastructure damage.

Additionally, the efficient use of natural resources, reducing carbon emissions, and improving energy efficiency in infrastructure management requires a well-trained and motivated workforce. Integrating sustainability principles into organizational practices must be supported by a high level of employee motivation and responsibility. Achieving resilience requires a continuous process of learning, adaptation, and innovation, with dynamic strategies that can respond to ever-changing environmental conditions.

And the last one is practical implementation of sustainable strategies for critical infrastructure management. To ensure the long-term resilience of critical infrastructure, the following measures and strategies should be implemented:

a) Investing in employee training and development: This includes both technical training on managing environmental risks and emergency response training.

b) Developing "green practices": Implementing sustainable technologies and practices in infrastructure operations, such as reducing energy consumption and using renewable energy sources.

c) Strategic planning for rapid response: Preparing disaster response plans with clearly defined roles and responsibilities for employees, as well as mechanisms for rapid infrastructure recovery after an incident.

By implementing these strategies, it will be possible not only to enhance the resilience of critical infrastructure but also to create a work environment where employees actively contribute to its strengthening and the preservation of environmental resources.

C. Effective Human Resource Management as a component of the Human Security's Environmental Dimension – In Search of Sustainable Solutions and Models

Undoubtedly, part of the challenges related to the overall shift in vision for sustainability in management processes in the areas already described is connected to the effective use of the human factor within these organizations. More than ever, finding key solutions is related to balanced and focused policies aimed at developing human capital [11].

This paper emphasizes some new aspects of human resource management that the authors have been working on in recent years, such as green HRM, the role of "green collars," and new ideas for employee motivation.

In this context, the role of effective human resource management in organizations managing critical infrastructure is examined, aiming to achieve sustainable results in areas related to environmental security.

Sustainable development requires an integrated approach where these three pillars are interconnected and mutually supportive within each organization and its organizational policies:

a) **Economic Sustainability:** This includes creating stable economic systems that support long-term growth and prosperity. Economic sustainability promotes efficient use of resources, development, and organizational stability.

b) **Social Sustainability:** This aspect focuses on improving the quality of life for people by ensuring access to education, healthcare, justice, and equality. Social sustainability also includes encouraging cultural diversity and participation in decision-making processes. This involves decisions in the area of "soft" skills and

competencies, which add value to the management and development of human resources.

c) **Environmental Sustainability:** Environmental sustainability aims to protect and restore natural resources and biodiversity. It involves reducing pollution, managing waste, and combating climate change with a comprehensive "green approach" in management.

The goal is to achieve a balance between them to ensure long-term well-being for both humanity and the planet. In Bulgaria, as in many other countries, the concept of sustainable development is integrated into national strategies and policies. For instance, Bulgaria's National Strategy for Sustainable Development (NSSDS) defines priorities and measures for achieving sustainable development in sectors such as energy, transport, agriculture, and tourism. It is important to note that sustainability is not just about environmental issues. It also includes social and economic aspects that ensure human communities can live in dignity without compromising their future resources. Sustainable development, on the other hand, is the path or process required to achieve this sustainability. Through this approach, the organization strives to ensure that the resources it uses today will continue to be accessible in the future, not only for the present but also for future generations [12].

Theoretically, since the 1990s, researchers have explored the role that human resource management can play in improving corporate environmental orientation, gradually focusing more on climate protection and introducing environmental management, driven by local air pollution, the first oil crisis, the water crisis [13], food crises, the first report of the Club of Rome, and others.

In the last decade, the need to integrate human resource management (HRM) with environmental management has become increasingly recognized, leading to the emergence of a separate branch in HR theory – Green HRM. The existing literature presents evidence of the impacts of GHRM indicators, the individual effects of human resource practices, or the impacts of overall high-performance work systems (HPWSs) on employee performance through several mediating mechanisms [14].

Two key psychological parameters can be identified as major influencing factors in Green HRM:

a) Environmental Knowledge: Awareness of the need to protect the environment increases the likelihood of eco-friendly behavior.

b) Environmental Psychological Climate: This climate signals that the organization supports eco-friendly behavior and attitudes, favoring eco-friendly behavior among employees, who align their workplace behavior with the adopted organizational culture [15].

To achieve green goals and environmental initiatives, organizations should:

a) Encourage a green image and develop recruitment processes that attract capable and motivated employees who share the organization's green values and principles.

b) Initiate processes and activities that motivate, engage, and encourage employees to participate in green initiatives and improve their green skills in the context of motivational processes.

c) Ensure that corporate values related to green goals are clearly communicated among employees.

d) Ensure that employees' green outcomes are appropriately monitored, recorded, and evaluated.

e) Link employees' contributions to green technologies with internal promotions and visibly support financial and non-financial rewards [5].

In the context of new challenges for HRM, attention must also be given to a particularly sensitive and new trend – the role of so-called green collars. These are employees directly involved in the activities of specific and particularly significant organizations and activities, including in critical infrastructure aspects. Green collar workers are responsible for jobs related to sustainability procedures and environmental protection in general. Green-collar workers, employed in every sector, emerged as businesses employed qualified experts, engineers, consultants, or managers in sustainability after the green transition and sustainable compliance in traditionally performed jobs. The green transition in the economy also brings about significant changes in employment and human capital. The characteristics sought in people to be employed in the green economy will differ. Green-collar workers are a group of employees born from the green economy [16].

The green economy approach has emerged alongside the concept of sustainable development. To achieve sustainable development, countries need to transition to a green economy and follow sustainable policies. Traditional economic approaches cannot provide any opportunity to implement sustainability policies in the long term [17].

An important aspect of the relationship examined by the authors between effective human resource management and environmental security, protection of human ecological rights, and the sustainability of critical infrastructure is the use of innovative approaches to motivating participants in these processes and relationships [18]. The complexity and challenges of the changing security environment provide the basis for finding innovative and sustainable models for motivation, including solutions related to new employee expectations that align with the evolving role of human capital in underdeveloped areas [19]. In this regard, some good practices can be pointed out in the field of "soft skills," which are becoming increasingly important for employees, including in the security sector. Finding a balance between work and personal time, between an individual’s needs and organizational goals, and balancing psychological and physical aspects of work are relationships that require new solutions, especially during times of acute and often

chronic crises and instability in entire sectors. Of course, this approach is linked to a clear regulatory framework and well-founded legal bases [20].

When changes are experienced as positive or well-aligned with core values, individuals may assimilate these changes into their identity, reinforcing a cohesive sense of self [21]. For example, the motivational model "Motivation 4.0" is one of the latest developments, widely applied in public sector organizations in recent years [22]. It combines four key motivation areas – Corporate Social Responsibility (CSR), Emotional Intelligence (EI), Green Human Resource Management (GHRM), and benchmarking/best practices and storytelling. The application of balancing policies and tools, according to the authors, leads in the short term to increased motivation by balancing employee needs, accepting the role and significance of their organizations in building a harmonious society. Although still new, the model has won awards in good practice competitions for public sector organizations, and interest in it is linked to its balance and easy adaptation to specific organizational conditions.

Certainly, it is worth adding another area that organizations should focus on in the coming years in search of balanced and distinguishing policies to position themselves as outstanding employers – specifically, policies related to employee well-being, which are linked to aspects beyond economic ones. There are three areas where, in recent years, there have been numerous good practices and policies – well-being, resilience, and mindfulness practices [23]. Holistically developed and systematically applied employee care policies ensure a sustainable increase in employee motivation on one hand, while on the other hand, enhancing their image as employers.

These challenges and solutions are of particular importance and potential opportunities for organizations in the sectors of environmental security, critical infrastructure, and the overall framework of national security. This focus in human resource management is likely to be critically important for balanced personal and career development and will attract more potential candidates to work in these institutions [24]. Of course, the fact that in the short term, the positive organizational climate and culture will significantly improve, which is a key characteristic in seeking sustainable solutions in such a significant sector as national security in recent years, cannot be overlooked.

III. Results and discussion

The topic of this research is highly relevant in the context of contemporary global challenges and the need for integrated solutions for environmental security and human resource management. The ability to protect human environmental rights and ensure the resilience of critical infrastructure is crucial in addressing growing climate threats and eco-economic crises. Technological innovations and new human resource management strategies, such as the concept of "green-collar" workers, play a vital role in ensuring the sustainability and adaptability of critical infrastructure under environmental risk conditions.

At the same time, the protection of human environmental rights is not only a moral and legal issue but also a key element of national and international policies that guarantee the safety and stability of society. This interconnection between environmental, social, and organizational aspects makes the topic particularly relevant and significant for modern scientific and managerial discussions.

New challenges in visionary management of critical sectors essential for sustainable development are increasingly becoming subjects of scientific and practical interest. In this context, the triad of "environmental security – critical infrastructure – human resources" is of great importance in the framework of national security.

IV. Conclusions

The balance between goals, plans, and results in a dynamic environment is part of an organization's sustainable development policies. On the other hand, it is maintained by that aspect of management functions, such as goal-setting, which is carried out in the interest of society in accordance with public and international values, rules, and norms.

A balanced approach to finding solutions within the triad of "environmental security – critical infrastructure – human resources" is a process necessary at the national level to transition from the current state to the desired state (i.e., to successfully move toward the future). It involves strategic decisions (which have a long-term nature) and strategic actions applied in formulating and implementing strategies that ensure coherence within the system and between the system and its surrounding environment, allowing for the achievement of set goals.

We will conclude with a beloved passage from *Alice in Wonderland*:

"Would you tell me, please, which way I ought to go from here? - Alice asked.

- That depends a good deal on where you want to get to - said the Cat.

- I don't much care where - said Alice.

- Then it doesn't matter which way you go - said the Cat.

- ...so long as I get somewhere… - Alice added as an explanation.

- Oh, you're sure to do that - said the Cat - if you only walk long enough…"

The challenges and possible solutions for efficiency within the triad of "environmental security – critical infrastructure – human resources" define both the path and direction of development. Part of this journey involves formulating a new vision for managing these relationships—one that seeks but also offers strong engagement, an emphasis on employee development, and long-term, sustainable solutions.

REFERENCES

[1] D. Sidova, "Политическата сигурност като измерение на свободата от страх в контекста на човешката сигурност" [Political security as a dimension of freedom of fear in the context of human security], Security and Defense Scientific Journal, Year II, Vol. 2, p. 153-154, December 2023, [Online]. Available: https://institute.nvu.bg/bg/statia/politicheskata-sigurnost-kato-izmerenie-na-svobodata-ot-strah-v-konteksta-na-choveshkata [Accessed February 10, 2025], https://doi.org/10.70265/ACKH6038

[2] See more in D. Sidova, "Human security concerns relating to environmental issues", Integration of the Western Balkans in NATO as a Guarantee for regional stability. Skopje: Center for International and Development Studies Skopje, ISBN 978-608-245-725-3, pp. 66-79, 2021.

[3] D. Sidova and Pr. Kostova, "Ecological security and environmental security – similarities and differences". International Scientific Journals of Scientific Technical Union of Mechanical Engineering "Industry 4.0", vol. 4, Issue 3, Sofia, Bulgaria, ISSN 2535-082X, pp. 91-94, 2020. [Online]. Available: https://stumejournals.com/journals/confsec/2020/3/91 [Accessed February 10, 2025]

[4] G. Kent, "Freedom from want: the human right to adequate food". Washington, D.C: Georgetown University Press, 2005. [Online]. Available: http://www.oda-alc.org/documentos/1341423652.pdf [Accessed February 10, 2025]

[5] N. Ilieva and V. Vasilev, "Green Human Resource Management and Sustainable Development: Insights from Bulgarian Organisations", Education of Economists and Managers, vol. 71, Issue 1, pp. 7-16, January-March 2024. [Online]. Available: https://econjournals.sgh.waw.pl/EEiM/article/view/4547 [Accessed February 10, 2025], https://doi.org/10.33119/EEIM.2024.71.1

[6] P. Arabadzhiyski, "Контрол на трудовите ресурси, обществените поръчки и финансите на малките и средните предприятия, осъществяващи охранителна дейност в Република България" [Control of labor resources, procurement and finance SMEs carried security in the Republic of Bulgaria], Collection of Scientific Reports of XXVI International Scientific Conference for Young Scientists, ISSN 1314-4669, p. 301, June 22-23, 2017. [Online]. Available: https://eprints.nbu.bg/id/eprint/4209/1/Statiq_rotated%20%281%29-2-9.pdf [Accessed February 10, 2025]

[7] Актуализирана стратегия за национална сигурност на Република България [Updated National Security Strategy of the Republic of Bulgaria]. Adopted by Decision of the National Assembly of 14.03.2018, published in the State Gazette, issue 26 of 23.03.2018. [Online]. Available: https://www.me.government.bg/files/useruploads/files/akt.strategiq2020.pdf [Accessed February 10, 2025]

[8] Национална Стратегия за адаптация към изменението на климата и План за действие [National Strategy for Adaptation to Climate Change and Action Plan]. Adopted by Ministry of Environment and Water of Bulgaria, p. 6-9, 2023. [Online]. Available: https://www.sp2023.bg/media/com_dpattachments/attachments/com_content.article/19RH621pr-12.pdf [Accessed February 10, 2025]

[9] Европейска комисия, Известие на комисията: "Технически насоки за климатична устойчивост на инфраструктурните проекти" [European Commission Notice: Technical Guidelines for Climate Resilience of Infrastructure Projects for the Period 2021-2027]. Adopted by National Association of Municipalities in the Republic of Bulgaria, p. 40-42, July 29, 2021. [Online]. Available: https://www.namrb.org/userfiles/V_pomosht_na_obshtinite/2-climate_proofing_guidance_bg.pdf [Accessed February 10, 2025]

[10] Устойчивост на критичната инфраструктура: по-строги правила, Критична инфраст-руктура: Комисията ускорява работата за изграждане на европейска устойчивост [Critical Infrastructure Resilience: Stricter Rules, Critical Infrastructure: The Commission Accelerates Efforts to Build European Resilience]. Press release from the official website of the European Union, October 18, 2022. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/bg/ip_22_6238 [Accessed February 10, 2025]

[11] S. Stoykov, "The system of education, training and research in the field of security - Managing change through experience and knowledge", ETR, vol. 4, pp. 269–274, Jun. 2024, https://doi.org/10.17770/etr2024vol4.8213

[12] A. Iddagoda and H. Dissanayake"The intervening effect of employee engagement on the relationship between high performance work practices and employee job performance", Three Seas Economic Journal, 3(2), 13-20, 2022, https://doi.org/10.30525/2661-5150/2022-2-2

[13] N. Dolchinkov, "Construction of a system for monitoring the pollution of water bodies with waste", ETR, vol. 1, pp. 136–141, Jun. 2024, https://doi.org/10.17770/etr2024vol1.7989

[14] E. Ari, O. M. Karatepe, H. Rezapouraghdam and T. Avci, "A Conceptual Model for Green Human Resource Management: Indicators, Differential Pathways, and Multiple Pro-Environmental Outcomes. Sustainability", 12(17), 7089, 2020. https://doi.org/10.3390/su12177089

[15] V. Dimitrova and P. Pavlov, "A new approach to sustainable management – the concept of social farming", ETR, vol. 1, pp. 116–122, Jun. 2024, https://doi.org/10.17770/etr2024vol1.7995

[16] S. Yıldırım and V. Vasilev, "The future of green collar workers: green transition in employment. In S. Yıldırım, D. Yıldırım, I. Demirtaş, & V. Kandpal (Eds.), Green Transition Impacts on the Economy, Society, and Environment" (pp. 1-16). IGI Global Scientific Publishing, 2024, https://doi.org/10.4018/979-8-3693-3985-5.ch001

[17] V. Vasilev, D. Stefanova, C. Popescu, "Human capital management and digitalization - from good practices and traditions to sustainable development", Book Chapter: Digitalization, Sustainable Development, and Industry 5.0: An Organizational Model for Twin Transitions, pp. 41–65, 2023, https://doi.org/10.1108/978-1-83753-190-520231004

[18] S. Drouin-Rousseau, A. J. S. Morin, C. Fernet, S. Austin and, B. Fabi, "A person-centered perspective on employees' human resource management values and their implication for organizational commitment.", Canadian Journal of Administrative Sciences / Revue Canadienne des Sciences de l'Administration, 1–16, 2024, https://doi.org/10.1002/cjas.175

[19] M. Temelkova and N. Bakalov, "Integrated Model of Production and Engineering Chains in Smart Manufacturing", Technologies in Industry 4.0. Engineering Proceedings, 60(1), 25, 2024, https://doi.org/10.3390/engproc2024060025

[20] M. Chochova, "Some Questions Regarding the Grounds and Procedure for Declaring the Invalidity of a Collective Employment Agreement." Yearbook of the Law Department, 10(11), 224–235, 2021, https://doi.org/10.33919/yldnbu.21.10.11

[21] H.M. Jerónimo, F.B. Tigre, P.L. Henriques et al., "Green work-life synergy? Exploring pathways from green HRM to organizational environmental performance." Rev Manag Sci, 2025, https://doi.org/10.1007/s11846-025-00855-4

[22] V. Vasilev, D. Stefanova, and M. Icheva, „Green human resource management as a component of sustainable organizational development in environmental and natural economics", ETR, vol. 1, pp. 402–407, Jun. 2024, doi: 10.17770/etr2024vol1.7966

[23] J. Tabor-Błażewicz, "Social Wellbeing in the Workplace: HR Activities and Impact", Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie 4(1002): 103–115, 2023, https://doi.org/10.15678/ZNUEK.2023.1002.0406

[24] R. Marinov, "Contemporary challenges to the protection of the country's sovereignty", ETR, vol. 4, pp. 168–172, Jun. 2024, https://doi.org/10.17770/etr2024vol4.8187

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference, 2025. Volume V, 29-35

Analysis of the Cold War for Public Opinion, and the Interests in the Cyberspace

Plamen Atanasov
New bulgarian university
Sofia, Bulgaria
atanasovp@abv.bg

***Abstract*— The research focuses on the interests involved in influencing public opinion both within one's own country and abroad. The advancement of globalisation and the intensification of informational connectivity make this topic increasingly relevant in the information-dominated world of the 21st century. Malicious access to the attitudes and sentiments of individuals is understood as a challenge to national security. The aim of the study is to uncover the broad scope, potential and the key factors involved in contemporary competition for access to public opinion, as well as some differences in state-level strategies. The focus is set on the cyberspace and on informational interventions, identified as a defining factor in today's international security landscape. The methodology is based on comparison and generalisation. The scientific approach is phenomenological. Accessible data has been used to define vectors for the presence of states in cyberspace. These are: software, hardware, and technologies, as well as artificial intelligence. Following a theoretical analysis, three defining vectors for public opinion were identified: mobility, ideological environment, and informational accessibility. A comparative analysis of the interdependencies between the identified vectors was carried out, considering the US, Russia, the UK, and the EU, as states of interest in international security. The analysis also includes the interests from cyberspace as an independent participant in this competitive interaction. The work reveals differences in the strategic approaches to accessing public opinion and to protecting it from unwanted manipulations. Furthermore, the study shows that, despite the differences, the competition for access to the attitudes and sentiments of individuals is associated with high costs, which are exhausting for society. The primary conclusion reached is that the competitive actions of the analysed actors resemble a New Cold War, fought for access to influence over public opinion in states. It is emphasised that in this New Cold War, more than two centres of influence are emerging. They "fight" in different ways, but resistance is inevitable and increasingly requires greater material and societal potential.**

Keywords*— *security, public opinion, Artificial Intelligence, New Cold war

I. Introduction

In the third decade of the 21st century, it is impossible for a state and its people to live isolated from other states and the societies within them. In the contemporary, information-dominated social connectivity, there is a clearly observable increase in the intensity of interactions, as well as in attempts to impose control over the channels through which influence is exerted in society, whether this influence originates from within the state or from another. A critical review of existing theoretical analyses and publications in authoritative media (listed in the References) reveals a clear trend towards the emergence of a specific competitiveness in today's international relations. Consequently, the uncertainties regarding the protection of one's own society from foreign influence are drawing increasing attention. It has been a well-known fact for decades that the active promotion of interests does not occur solely between societies in countries with shared borders. Today, this fact is more evident than ever before. The rapid development of cyberspace and its capabilities leads to the emergence of increasingly new effects in the relationship between information warfare and interventions in public sentiments and attitudes. The relevance of these uncertainties is indisputable and requires increasingly active research efforts. In line with the emerging needs, the objective of this study is to reveal the growing potential for the exertion of foreign influence in the society of another state, as well as to highlight the strategic approaches to competition among some of the leading political and economic powers. The study focuses on the possibilities for individually addressing participants and balancing the ongoing processes in the realm of public diplomacy and international security.

In the context of security, the topic is of significant relevance because the history of social development

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8510
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

allows us to view the state as a system that society within it has constructed in order to achieve security [1]. This system operates both with its internal processes and with those triggered by its interaction with the surrounding environment. Security in such systems is multi-faceted and is supported by two main pillars: physical (state borders, economic factors, etc.) and moral, which is entirely positioned within the thinking of people and, more precisely, in the worldview they 'paint' in their minds, and then transfer into their pursuits, demands, and agreements for the order and policies of the state they live in [2], as well as the actions of other states (other systems) with which they interact. This transfer is particularly dependent on public opinion and has become an increasingly important factor for international security. Especially now, when 'The information age has changed the practice of existing security systems by making them operate in a rich information environment, creating and implementing a number of new complex policies.' [3]

Public opinion is the construct that unites people within the framework of social agreements. Within this unification, people impose their shared interests, thus shaping the activity of the state. Therefore, public opinion exerts a decisive influence on both the domestic and foreign policy of the state. For this reason, protecting society from the penetration of foreign interests is an especially important element for the security of the state. On the other hand, promoting one's own interests within the society of another state facilitates agreements on various issues and serves as a powerful prerequisite for resolving conflicts without bloodshed. Therefore, public opinion is an interesting construct in the context of security. The drawback is that this construct is described more qualitatively than quantitatively, which significantly complicates not only scientific research but also the practice of conducting and safeguarding against interventions.

Regarding public opinion, the historical development in Europe, and later in the world, shows three important vectors in public development, which are connected to the following periods: The first are the wars for the imposition of Catholic power in Central and Western Europe. During the Hundred Years' War (1337–1453), people participated in the war, left their settlements, and met other people, other cultures, and the way of life of their close and not so close neighbors. In addition to fighting, they encountered different cultures, learned different ways of farming, trading opportunities, and so on. In 1454, Johannes Gutenberg published the first printed book. Even after the war, people sought ways to travel, to maintain connections outside their settlement. The collective energy of the communities was awakened. A logical factor for this development is mobility.

Social development continues. By the early 17th century, there is no doubt in Europe about the development of society. It is then that the first newspapers appear, and it becomes clear that not only movement is important, but also the ideas that are transferred. It is evident that the intensification of communication has the advantage of promoting the spread of one's own ideas, but it also has the disadvantage of "opening the doors" to the spread of foreign ideas within one's own society. These ideas are not always in the interest of the people and the authorities. Combining them with public activity that emerges among the people, presents a powerful challenge. The Catholic Church finds a way to refine the spread of faith by developing the tool of propaganda (in 1622, the *Sacra Congregatio de Propaganda Fide* was established). Thus, ideology and the freedom of ideas emerge as the next defining vector for public opinion.

By the middle of the 20th century, society had changed to such an extent that physical armed conflicts became increasingly difficult to carry out and inflicted heavier and heavier damage. The era of the Cold War began in interstate relations. It is commonly associated with blocking potential by developing and producing weapons, the potential use of which mutually blocks the initiative of states. It should not be underestimated that the Cold War was also a war between the ideologies of the two opposing camps – the East and the West. While the produced weapons were not used, battles on the ideological front continued in full force. These were battles for attracting public opinion in support of the interests of the intervener (the offensive actions of the opponent and the defensive actions of one's own state).

In the 21st century, the world is different. The arms race has been abandoned, but competition between systems in the direction of public opinion remains. Mobility, especially among young people, is highly developed. They travel to work, to study, and to get acquainted with the culture and everyday life of people in other countries. This creates the need to develop a "suitable environment for intercultural communication". [4] The strategic dimensions of the culture-society complex are increasingly drawing thinking within the field of security. [5]

One of the reasons is the advanced globalization. An example of this are the crises. In the 21st century, there is no doubt that it is impossible for a single country and its society to deal with the unknowns related to transportation between countries [6], climate, energy exchange, and distribution [7], etc. Because of this, the questions today are not how public opinion is formed, but how to achieve understanding between public opinions in different countries. Against the backdrop of these developments, it is not surprising that in the 21st century, social development is expanding into a new environment – cyberspace. Even a brief look at this novelty makes cyberspace an important vector for shaping public opinion [8]. In accordance with established concepts in science and practice regarding the structure of cyberspace, it can be divided into: software, hardware, and another construct that has emerged in recent years – artificial intelligence.

The race for control over the movement of people and the spread of ideologies are 'historically developed' activities. As an innovation in the race for access to public opinion in the direction of cyberspace, another specific structure should be considered. This construct influences public opinion in different countries, but it is not a state. It

is also not clear on what interests it operates. These are those actors in the security ensemble who have the ability to block connectivity, stop profiles on social networks (as happened, for example, with the profiles of U.S. President Donald Trump and his supporters during the transfer of power in 2021), activate or suppress public opinion, initiate or block initiatives on social networks, or stop some and launch other informational websites. From a security perspective, such interventions are far from harmless. In the case of the events at the Capitol, the intervention seems positive, but this is not always the case. For example, in 2018, software robots blocked images of the Venus of Willendorf – a figurine in the Natural History Museum in Vienna, known as the oldest exhibit of paleontological art. The reason given was that the figurine was nude [9]. As a result, millions of people around the world could not see the image and were essentially cut off from access to culture. The question arises: who is working with these software robots? Another question concerns the public appropriateness of the actions of those who control the exchange of information in cyberspace. These actions resemble censorship, the control of which is unknown, and it is unclear whose interests are being served. When considering the effect of determining which news is real and which is fake, which ideas on social media are dangerous and which are not, it becomes evident that there is a huge potential for interventions into public opinion. A potential that remains hidden from society. The actions of these actors, hidden in cyberspace, may seem virtual, but they are tangible, and it is not correct to ignore them when describing the current landscape of international security relations. The working term used for these actors is "supranational entity."

II. Materials and Methods

A phenomenological scientific approach has been applied. It is based on experience and the perception of the world. On this basis, it can be seen that the historical context in social development proves that public opinion is an important element in relations between states and is a crucial factor for international security.

The methodology is based on comparison and generalisation. Available publications in scientific journals, as well as in authoritative global media, have been examined. These were selected in the context of the investigated issues. This allows for the identification and comparison of the main differences in the strategic approaches of the United States, China, Russian Federation, EU countries, and the United Kingdom. Moreover, it reveals the reasons behind the discovered differences in strategic approaches. In terms of quantitative analysis, as much as possible, a comparison was also made of the expenditures these countries allocate to implement their policies. These methods of comparison and description allow for the synthesis of the conclusion that we are witnessing activity resembling Cold War dynamics. In accordance with the research problem and the set objective, the results achieved reveal the potential of activities aimed at accessing public opinion. Furthermore, they provide a broad response to the question of possible actions to protect society from malicious foreign influence via cyberspace.

III. Results and Discussion

The experience of the centuries, as well as today's information-dominated reality, create a sufficient foundation for formulating the vectors that simultaneously act towards the protection of public opinion from foreign interventions, as well as the imposition of interests through the 'capture' of foreign public opinion. Such vectors are:

1) Towards public opinion
– Mobility;
– Freedom of ideas;
– Informational connectivity between people within the state and with people from other countries' societies;
2) The state's potential in cyberspace:

- The level of development of software and
- The level of development of hardware
- Activity in building accessible civilian applications of artificial intelligence.

The corresponding vectors are analyzed for: the United States, China, Russian Federation, EU countries, and the United Kingdom, as well as the supranational entity that manifests itself through cyberspace. The states are chosen according to the established view in European media of the leading states in the geopolitical future [10]. The vectors are assessed as follows:

1) Regarding public opinion:

- Mobility: according to the widely known conditions regarding the existence of restrictions on people's ability to travel outside the country;
- Freedom of ideas: according to the degree of freedoms in the direction of the established values in Western European thinking;
- Informational connectivity: according to the known data on individual internet consumption. [11]

2) Regarding the state's potential in cyberspace:

- Software: according to known data about the localization of major companies that own operating environments;
- Hardware: according to known information about hardware dominance in building the internet connectivity network;
- Artificial intelligence: according to known developments and influence in platforms like ChatGPT and other similar ones.

The indicators are assessed in three categories: high, medium, low. The evaluations are in the context of the possibilities for influencing public opinion and should not be applied as exhaustive for the presence of the analysed states in cyberspace.

The obtained result is presented in Table (1).

TABLE 1:REGARDING STATES: MOBILITY, FREEDOM OF IDEAS, AND THE POTENTIAL FOR INTERVENTION THROUGH CYBERSPACE.

State	Mobility	Freedom of ideas	Individuals using the Internet	Software	Hardware	Artificial Intelligence
USA	high level	high level	high level 89.4%	high level	middl	high level
Russian Federation	high level	low level	high level 82.6%	low level	middl	middl
China	high level	low level	middl 64.6%	middl	high level	high level
EU and United Kingdom	high level	high level	high level 83.8% (UK – 92.5%)	middl	middl	high level
Superstate subject	?	?	56% (in the world)	high level	high level	high level

USA: The freedom of travel for American citizens is well-known. The existence of a democratic environment in the country is also well-known. The high level of software power is due to companies like Microsoft and Apple. Regarding hardware, some difficulties are observed. An example is the disputes with China over equipment for 5G networks.[12]. The public use of artificial intelligence is associated with the development of ChatGPT.

Russian Federation: There is no data indicating total restrictions on the mobility of Russian citizens. However, the freedom of ideas is in question. A notable example is the well-known case of Russian opposition leader Alexei Navalny. Regarding hardware for informational connectivity, the Russian initiative RuNet, which aims to control the entry and exit points of the internet in the country, deserves attention. [13], [14]

China: Chinese tourists are increasingly encountered around the world. This is grounds for evaluating the level as high. Regarding the freedom of ideas, a low level is noted due to concerns about the imposition of restrictions by the typical communist capitalism that the country develops. Regulations imposed by institutions via the internet (e.g., social networks) are also well-known. The software level is rated as medium, but the hardware level is high. This is due to the equipment that China manufactures and supplies to other countries, such as for the 5G network. After the emergence of DeepSeek, the influence level through artificial intelligence is high. These are characteristic policies of the state.

EU and the United Kingdom: The freedom of travel for citizens from these countries is widely known. The democratic environment in these countries is also well-known. The software presence is not low due to the activity of developing open-source software, such as Linux. Regarding the production and implementation of hardware, difficulties are observed. The activity of developers from these countries in limiting undesirable effects and threats from uncontrolled and thoughtless application of artificial intelligence is well-known.[15]

Supranational entity in cyberspace: Due to the lack of physical borders, physical mobility cannot be discussed. Regarding the freedom of ideas, it is questionable whether the neoliberal permission for everyone to write whatever they want creates a democratic environment. The level of software presence is difficult to determine. It is assessed as high because it utilizes all the available software resources on the planet. Regarding hardware, the assessment is high, as it is clearly under the control of the supranational entity. Regarding the public use of artificial intelligence, it is difficult to form an opinion, although there are doubts about interventions in the generated texts. However, it is not known in which direction these interventions occur. [16]

The first type of policy that emerges is that: The focus on public opinion is evident in each of the studied units. All the studied countries strive for a high level of mobility for their citizens, but some apply visa or similar regimes (e.g., USA, United Kingdom, etc.), i.e., they limit visitation.

The second type of policy is that: While some countries protect public opinion from unwanted interventions by developing democratic freedoms and ideas (e.g., USA, EU, and United Kingdom), others impose restrictions on some of these vectors (China, Russian Federation).

Both policies are remnants of the era before the emergence of cyberspace, but they are clearly still exploited today. They remain as options for protecting public opinion in their own countries.

The third type of policy is strictly oriented towards influencing public opinion through cyberspace. Technologically, it relies on mutual compensation across the vectors of software, hardware, and public use of artificial intelligence. This policy is highly relevant in the everyday life of the 21st century. This is evidenced by the fact that, in the context of the typical information dominance of the 21st century, leading states in geopolitics maintain levels of individuals using the Internet that are significantly higher than the global average. This indicates that, in the 21st century, a substantial part of the competition for access to public opinion takes place through cyberspace. In the realm of international security, presence in cyberspace proves to be a prerequisite not only for protecting public opinion from external influence but also potentially for influencing the societies of other countries. This situation explains the high interest of states in the vectors of software, hardware, and artificial intelligence. The three vectors mutually compensate each other. In cases where a state does not have high control over the software of the operating environment, it prioritizes the development of hardware devices, as seen in China.

The research demonstrates that the combination of the vectors of ideological freedom/restriction and/or mobility

with interventions in cyberspace is primarily employed by developed nations and affects people worldwide. It is reasonable to assume that, within the framework of their capabilities and political order, other countries around the world also implement such policies. Therefore, the focus is placed on interventions in cyberspace. This is further evidenced by the expenditures made by states.

According to available data on the internet, the costs directed toward the third type of policy are substantial. For example, US investments in ICT (Information and communications technology) in 2024 are $560.95 billion [17]. The country's GDP for 2024 being $29,179.1 billion USD [18]. In the same year, global ICT spending is $4,997.718 billion USD [19]. This means that more than 10% (11.22%) of the global ICT spending comes from the USA. It is not easy to find data for other countries, nor can we be sure that these data are comparable, but judging by the available media reports, the ratio is similar to that of the USA. This shows that for leading countries, a significant portion of expenses is directed towards ICT. These expenses are a substantial part of GDP, as seen from the data for the USA. The circumstances resemble the situation during the Cold War in the 20th century.

According to the described conditions, a New Cold War for public opinion emerges, which is being fought in cyberspace. In this conflict, the poles are more numerous, and the interests are more complex. Furthermore, it is widely known that reaching public opinion occurs through various means: cyberattacks against corporations and institutions; information theft; trolls who fabricate interference in parliamentary and other types of elections; propaganda messages aimed at attracting public attention through fake news, deepfakes, and false messages in online-based social networks; as well as other methods. The diversity is substantial, both in terms of the participants and the affected parties, as well as the tools used. This complicates efforts to limit malicious influences on society that are propagated through cyberspace. Additionally, cyberspace is visibly evolving at speeds disproportionately higher than the legislative processes in democratic countries. As a result, when a tool is restricted by laws or technical countermeasures, cyberspace technologies swiftly create a new tool to replace the restricted one.

In the context of this vision, an interesting element in the policy for the public implementation of artificial intelligence (such as ChatGPT and DeepSeek) is that countries like Russian Federation are not highly engaged in such a race. The data available in open sources about the scale of Russian investments in the fields of software, hardware, and artificial intelligence is incomplete, and it is unclear how reliable it is. This does not mean that Russia is not working towards artificial intelligence. However, this expansion remains in the background, likely due to the comfort created by limited democratic freedoms. A different situation is developing in China. The difference is that the authorities in China are developing both artificial intelligence and internal connectivity between citizens, while simultaneously imposing strong control over citizens' presence in cyberspace. Users are required to register with their real names (no nicknames), confirmation is needed through personal ID, phone numbers, and even social credit numbers [20], [21].

The policy of the supranational entity is not fully known. It is composed of a group of people who, due to ownership or their professional skills and positions, manage, administer, resolve, and restrict access to information on social networks, websites, etc. The organization of the internet network is such that it is difficult to assess the capabilities of people within this group. Their policy is unique because it is entirely conducted in the domain of the complex: software, hardware, and the use of artificial intelligence in the public sphere. The challenge is that it is unclear who is behind this supranational entity and what interests it defends. It is also unknown to what extent it holds influence and control over internet connectivity between people.

In this line of reasoning, the activity of British experts engaged with cyberspace is of particular interest, as they advocate for international agreements concerning the rules for publishing and disseminating information via the internet. In such a scenario, the supranational entity in cyberspace would become visible, and its activities would be brought into alignment with societal rules and laws. This would have an important effect. However, how states will balance and negotiate their interests is a complex question, one that goes beyond the scope of this report. It can be argued that such an agreement is not only possible but also necessary, and it is not feasible for states to remain indifferent to this evident fact. Moreover, there is little doubt that the need for institutions, corporations, and individual users to maintain and update their protection against cyberspace aggressions remains essential. However, this is again linked to increasing investment.

Against the backdrop of the uncertainties and challenges associated with developing normative protections for public opinion against interventions, technical countermeasures emerge as an interesting possibility. This direction is exemplified in the policy of the Russian Federation, which is developing technical restrictions on the country’s internet network. Similarly, the development of indigenous artificial intelligence (e.g., ChatGPT and DeepSeek) appears to be following this trend. Such a solution is also not straightforward, and an important feature is that it requires ever-increasing resources that states must allocate in one way or another. Making such large expenditures is draining and may eventually come at the expense of social benefits and other priorities. In this regard, the argument becomes clear that the competition for supremacy in cyberspace is not merely a race for dominance in a new domain of competition, but a far more encompassing phenomenon. A phenomenon that approaches the understanding of a New Cold War.

CONCLUSIONS

The results clearly indicate that active competition for dominance over the tools used to reach societies within states worldwide is developing in cyberspace. The reason is that dominance in cyberspace provides a significant advantage for influencing public opinion and steering it towards the interests of the intervener. This advantage is employed alongside other mechanisms, which adds a certain hybridity to the activity aimed at influencing public opinion. The phenomenological view of history allows for the identification of leading vectors in the social development of society, focusing on: mobility, ideological freedoms, and communication connectivity for the exchange of messages (information, ideas, etc.). The high significance of the effects necessitates active research on the issues, leading to direct outcomes in the field of social sciences and security.

In the 21st century, the emergence and development of cyberspace place humanity in an increasingly higher dependence on Information and communications technology. This shapes the vectors: software, hardware, and artificial intelligence.

The report demonstrates that policies regarding public opinion, as well as control and manipulation concerning mobility and ideological freedoms, have not been abandoned. It is still used to maintain public opinion within a state and to protect it from foreign interference. This means that actions are required to regulate the activity of accessing and publishing information, both at the international level and within the state's internal framework. The research outlines the challenges but reaches the firm conclusion that international regulation is necessary, both in terms of the content of the information exchanged through cyberspace and with regard to dominance in internet infrastructure. However, achieving such regulation does not absolve organisations and individual users from the responsibility of maintaining adequate levels of software protection.

Alongside the work on established vectors such as mobility and ideological freedoms, ICT is developing in a direction where supremacy is sought within the framework of the software, hardware, and public access to artificial intelligence complex. Different components of the complex are used in various combinations. For example, when a state is not leading in software, it focuses on hardware devices and connectivity networks. Artificial intelligence is the third factor in which competition develops dynamically. The high costs of protection, combined with the strong interest in influencing public opinion through cyberspace, provide grounds to suggest that an activity is emerging that closely resembles the principles of the Cold War – economic exhaustion at the expense of maintaining parity between leading centres. Unlike the well-known Cold War, which ended in the 1990s, today's activity is characterised by multi-vector dynamics and more than two centres. This makes international agreements even more complex.

Investments in ICT, as well as policies in leading countries, provide grounds for the hypothesis that a New Cold War is emerging, one that is developing in cyberspace and is fought for access to people's thoughts and ideas. It affects the complex: software, hardware, and artificial intelligence.The research demonstrates that the importance of the issue should be outlined both theoretically and practically, by examining the nature of the processes and seeking not only the protection of one's own society but also counteraction against the race in cyber investments. One possible solution is for states to develop their own hardware and software to protect critical assets (as seen in the policy of the Russian Federation), but to what extent and for whom this is feasible is a question with multiple answers.

Today, attention should be given to the fact that the development of a New Cold War for dominance in cyberspace is possible, and states and the societies within them must not allow this to happen.

REFERENCES

[1] B. Buzan, O. Wæver and J. de Wilde. Security:a new framework for analysis. Colorado, London: Lynne Rienner Publishers, Inc., 1998.

[2] W. Lippmann. Public Opinion. New York: Harcourt, Brace and Company, 1922.

[3] S. Stoykov, R.Marinov and S. Dimitrova. The development of educational capacity of human resources in the field of security-main priority of national security, International Conference on Creative Business for Smart and Sustainable Growth, CreBUS 2019, March 2019, Article number 8840062, Category number CFP19U17-ART; Code 152084. [Online]. Available: DOI:10.1109/CREBUS.2019.8840062.[Accessed Feb. 12, 2025].

[4] Т. Вълова. Обучението по български език като втори на студенти по медицина – исторически и съвременни ракурси (Teaching Bulgarian as a Second Language to Medical Students – Historical and Contemporary Perspectives). Сборник доклади от научна конференция „80 години Съюз на учените в България". София, 2024, стр. 221-224.

[5] D. Berchev . The Past and the Future of European Union Strategic Culture and Thinking in the Field of Security and Defense. *Security and Defense*(1, June 2024), 25-49. [Online]. Available: https://institute.nvu.bg/sites/default/files/inline-files/2024-1-02-berchev.pdf. [Accessed Feb. 12, 2025]

[6] D. Dimitrov and I. Manchev. Methodolical and Tehnical Aspects of Models foe Digital Management of Transport Systems. In: ENVIRONMENT. TECHNOLOGY. RESOURCES. Proceedings of the 15th International Scientific and Practical Conference on June 27th–28th, 2024. Volume II, I: Rezekne Academy of Technologies, Rezekene, Latvia, 2024, pp. 79-82

[7] N. Dolchinkov. Optimizing Energy Efficiency in the Conditions of a Global Energy Crisis. In: Optimizing Energy Efficiency in the Conditions of a Global Energy Crisis. IGI Global, 2023. [Online]. Available: DOI: 10.4018/979-8-3693-0400-6, pp. 1–9. [Accessed Feb. 12, 2025]

[8] C. Painter. The rise of the internet and cyber technologies constitutes one of the central foreign policy issues of the 21st century. The Foreign Service Journal, June 2018. [Online]. Available: https://afsa.org/diplomacy-cyberspace [Accessed Feb. 12, 2025].

[9] H. Fohringer. Prehistoric 'Venus' statue too hot for Facebook. Artdaily.com, 2018. [Online]. Available: https://artdaily.cc/news/102827/Prehistoric—Venus--statue-too-hot-forFacebook. [Accessed Jan. 12, 2019]

[10] International relations. China, Russia, the US and the future of geopolitics. The Economist Education. [Online]. Available: https://education.economist.com/courses/internationalrelations?utm_source=economist&utm_medium=digital-house-

ads&utm_campaign=us-elec-camp-refresh-01-25 [Accessed Jan. 12, 2025].

[11] Individuals using the Internet (% of population). World-statistics.org. [Online]. Available: https://world-statistics.org/index-res.php?code=IT.NET.USER.ZS?name=Individuals%20using%20the%20Internet%20(%%20of%20population)#top-result. [Accessed Feb. 12, 2025].

[12] Т. Лахан. "Как малка Латвия се опълчи на Китай" („How small Latvia stood up to China"). DW, 2021, Dec. 15. Online]. Available: https://p.dw.com/p/44IbQ. [Accessed Feb. 12, 2025].

[13] С. Белова и А. Рассохин. „Суверенны интернет" переходит в фазу тестирования- Сможет ли Роскомнадзор полностью отрезать российский интернет от остального мира? ("Sovereign internet" enters the testing phase – Can Roskomnadzor completely sever the Russian internet from the rest of the world?). КоммерсантЪ, 24.09.2019. [Online]. Available: https://www.kommersant.ru/doc/4103277. [Accessed May. 10, 2022]

[14] "Русия блокира Фейсбук в цялата страна, спря и достъпа до Туитър" („Russia has blocked Facebook across the entire country and also restricted access to Twitter"). Vesti.bg. 04.03.2022. [Online]. Available: https://www.vesti.bg/sviat/rusiia-blokira-fejsbuk-v-cialata-strana-spria-i-dostypa-do-tiutyr-6139076. [Accessed Sept. 22, 2022].

[15] P.Guest. Inside the AI back-channel between China and the West. Computer scientists are reaching out across the geopolitical divide to try to stop an apocalypse. The Economist, Nov. 29th 2024. [Online]. Available: https://www.economist.com/1843/2024/11/29/inside-the-ai-back-channel-between-china-and-the-west. [Accessed Feb. 12, 2025].

[16] P. Atanasov. Persuasion potential: assessment through differences between the complexity of texts, generated with ChatGPT 3.5, and texts from traditional media. 2024 International Conference on Information Technologies (InfoTech-2024), 2024. [Online]. Available: DOI: 10.1109/InfoTech63258.2024.10701330 . [Accessed Feb. 12, 2025]

[17] Straits Research. "ICT Investment in Government Market Size". [Online]. Available: https://straitsresearch.com/report/ict-investment-in-government-market. [Accessed Feb. 12, 2025].

[18] "United States (USA) GDP - Gross Domestic Product". [Online]. Available: https://countryeconomy.com/gdp/usa?year=2024. [Accessed Feb. 12, 2025].

[19] Gartner. "Gartner Forecasts Worldwide IT Spending to Grow 6.8% in 2024". [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/01-17-2024-gartner-forecasts-worldwide-it-spending-to-grow-six-point-eight-percent-in-2024. [Accessed Feb. 12, 2025]

[20] L.He. China to punish internet users for 'liking' posts in crackdown after zero-Covid protests. CNN, Nov. 30 2022. [Online]. Available: https://edition.cnn.com/2022/11/30/media/china-new-internet-rule-punish-liking-posts-intl-hnk/index.html. [Accessed Feb. 12, 2025].

[21] M. Murgia and A. Gross. Inside China's controversial mission to reinvent the internet. FT Magazine.March 20 2020. [Online]. Available: https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f. [Accessed Feb. 12, 2025].

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 37-41

Environmental Protection and the New Safeguards Provided in Directive (EU) 2024/1203 on the Protection of the Environment Through Criminal Law

Daniela Atanasova
Public Law Department
South-West University "Neofit Rilski"
Blagoevgrad, Bulgaria
adv.atanasova@mail.bg

Nadezhda Krasteva
Public Law Department
South-West University "Neofit Rilski"
Blagoevgrad, Bulgaria
nkrusteva@law.swu.bg

***Abstract* — The research carries out an in-depth analysis of Directive (EU) 2024/1203 of the European Parliament and of the Council of 11 April 2024 on the protection of the environment through criminal law and replacing Directives 2008/99/EC and 2009/123/EC as a normative instrument for criminal environmental protection within the European Union. The Directive is a reaction to the growing environmental crime with a transnational dimension, requiring complex and modern measures for prevention and punishment. The main practical challenges arising from the transposition and application of the Directive are outlined. The conclusion of the study underlines that in order to achieve the objectives of the Directive and the effectiveness of the measures envisaged, it is not only necessary to harmonize legislation, increase the capacity of law enforcement and investigative authorities and enhance international cooperation, but it is essential to develop standardized investigative methods in relation to the different environmental crimes, taking into account their specificities. Efforts in this direction are indeed worthwhile, because the objective pursued is the protection of the environment, so important to our existence.**

Keywords* — *criminal protection, Directive, environment, protection measures

I. Introduction

To date, humans are already indebted to the environment, which has responded appropriately with a series of escalating natural disasters that have claimed thousands of lives and caused untold economic, social and security dimensions. The satisfaction of inexhaustible human needs at any cost, through the limitless extraction and pollution of natural resources, are among the main causes of the breakdown of the links between the various components of the environment that ensure ecological balance.

According to reports from a number of global organizations such as the UN, WHO, UNESCO, etc., over 2 billion people in the world now live in areas affected by a lack of clean drinking water [1]. Every year, millions of people die from waterborne diseases, more than all forms of violence combined [2]. A number of scientists are signaling that we are in the sixth major species extinction due to human activity [3]. And the disrupted ozone layer in the Arctic is the cause of melting ice, according to a 2020 study published in Nature Climate Change. Pollutants deposited on land and in soil are also a global problem, with airborne and waterborne pollutants found even on the highest peaks and most remote beaches. Although some pollutants break down in the soil over time others remain forever and inevitably affect people's lives.

As early as October 1972, the Paris European Council stated the need for Community political decisions and an environmental action programme to accompany economic development. As a result of the decisions taken, multiannual "environmental action programmes" have been drawn up since 1973 and continue to this day, with the right of citizens to a healthy and favorable environment as a fundamental principle during this period. To date, European legislation has undergone considerable development. Hundreds of regulations have been adopted governing the use of natural resources and the protection of the environment [4]. Moreover, even Article 3(3) of the Treaty on European Union (TEU) and Article 191 of the Treaty on the Functioning of the European Union (TFEU) guarantee the European Union (EU) a high level of

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8489
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

protection and improvement of the quality of the environment.

The emerging need for stricter measures to protect it has also led to the adoption of a Directive on the protection of the environment through criminal law. This was the first Community law act to contain requirements for the harmonization of criminal policy. Its adoption was prompted by the increase in environmental crimes and their consequences, which extend beyond the borders of the countries where they are committed.

In 2021, the European Commission, as a commitment to the Green Pact and in response to the ineffectiveness of existing environmental sanctions, adopts a proposal for a new directive on combating environmental crime, adopted on 11 April 2024 and replacing Directives 2008/99/EC and 2009/123/EC.

It is the analysis of this new directive that is the subject of this study, as a guarantee for more effective criminal protection against serious environmental violations in the EU.

II. Materials and Methods

The research is a theoretical and legal study of Directive (EU) 2024/1203 of the European Parliament and of the Council of 11 April 2024 on the protection of the environment through criminal law. The chosen objective is to bring out the strengths and weaknesses of the commented legislative solution with a view to effective environmental protection. In order to achieve the aims and objectives of the research, the method of scientific analysis and synthesis, comparative legal method, as well as various methods of interpretation of the legislative text have been used. The comparative law method used aims to provide a clear analysis of the key features of Directive (EU) 2024/1203 compared to previous legislation and to assess its effectiveness as well as the prospects for transposition into national legal systems.

III. Results and Discussion

Directive (EU) 2024/1203 is the result of the EU's efforts to provide criminal protection for the environment by applying common principles, objectives and sanctions to increasingly complex forms of offences. It introduces minimum rules on the definition and sanctioning of criminal environmental offences.

The main objectives of the Directive relate to:

1. Extending the scope of criminalized acts to reflect the most serious breaches of EU environmental legislation.

2. More precise definition of specific environmental crimes and harmonization of the type and level of penalties in EU Member States.

3. Stronger, effective, proportionate and dissuasive penalties, accessory sanctions (for environmental restoration) and measures for confiscation of funds and proceeds of crime.

4. Establish a clear and effective framework for law enforcement and cross-border cooperation in the fight against environmental crime, with a view to greater effectiveness in the detection, investigation, prosecution and sentencing of environmental crime.

The EU's objectives aim to achieve a high level of environmental protection and improvement. Measures taken by Member States to transpose them into national legislation should comply with the basic principles enshrined in EU environmental legislation - the "precautionary principle", the "preventive action principle", the "priority at source principle" and the "polluter pays principle".

Directive (EU) 2024/1203 is undoubtedly a step forward in environmental protection in the European Union, building on the directives it repealed. The objectives set imply a more effective counteraction to environmental crime and an increase in the likelihood of detecting and punishing offenders.

In this research, an in-depth analysis of the framework and the requirements it sets for the Member States is carried out. The aim is to highlight both the positive aspects of the Directive and its shortcomings which could hinder the achievement of a high level of environmental protection. The analysis has been carried out on the basis of the objectives it sets and their possible achievement.

1. Extension of the scope of criminalized acts

Directive (EU) 2024/1203 has significantly extended the scope of criminalized acts. It includes new offences covering a wider range of activities constituting serious environmental offences – pollutant discharges, illegal waste management, illegal marketing of products, damage to ecosystems, deforestation, invasive species offences, ship-related offences, etc.

In order to constitute a criminal offence, all these activities must be carried out in violation of the rules laid down in one of the European Union's regulations governing the use of natural resources, environmental protection and other parts of environmental legislation. Acts committed intentionally and with gross negligence, by act or omission, are criminal. Incitement and aiding and abetting, as well as attempt to commit the offence, are punishable for certain offences.

The criminalization of negative impacts on more of the components of the environment (air, water, ecosystems, wild flora and fauna, etc.) compared to Directive (EU) 2008/99 EC ensures more effective protection of the environment as a whole. On the other hand, the description of the environmental damage to the component concerned, as an element of the offence, means the identification of this damage by the investigating authorities, with all the difficulties that this entails.

An indisputable contribution and a positive aspect is the differentiation of administrative offences from criminal offences, with the development of clear criteria for this –

the requirement to derive a quantitative and qualitative threshold.

This threshold has been proposed to be in line with the constitutive harm that has occurred [5], which for an offence must be "substantial". This notion is not clarified, but the Directive sets out certain elements to be taken into account when assessing various environmental crimes and environmental components, namely: the baseline state of the affected environment; whether the harm is long-term, medium-term or short-term; its extent and reversibility; what the relevant regulatory threshold is and how many times it is exceeded; the conservation status of the species affected; the costs necessary to restore the environment, etc.

The Directive also provides for qualified offences for some of the criminal infringements leading to catastrophic consequences. Again, the criterion is ecological damage, but this time in terms of: destruction or widespread and significant damage that is irreversible and long-lasting to an ecosystem of significant size or significant ecological value, or to a habitat within a protected area, or to air, soil and water quality.

A significant contribution to the fight against environmental crime is the requirement to criminalize acts committed despite a permit issued by a competent authority, if that permit was obtained through fraud, corruption, extortion or coercion, or if it was issued in clear violation of the requirements for their issuance. The criminalization of the abstraction of surface water and groundwater, where significant damage is caused or is likely to be caused to the ecological status or the ecological potential of surface water bodies or to the quantitative status of groundwater bodies, is of fundamental importance with regard to water as a natural resource.

Criminalizing activities such as the introduction, spread, cultivation, release into the environment, etc. of invasive species also provides more effective protection for biodiversity.

In view of the foregoing, extending the scope of criminalized acts to the components of the environment adversely affected would contribute to more effective protection. Protection from excessive abstraction of surface water, for example, will always also provide protection for hydrobionts, flora, soil, etc. (even humans) in view of their interconnectedness.

However, criminalizing multiple acts without effective enforcement would not achieve the desired goal [6], [7].

2. A more precise definition of specific environmental crimes and harmonization of the type and amount of penalties in EU Member States

Achieving more precise definitions of the different types of environmental crime and harmonizing the law across the EU is a laudable objective of Directive (EU) 2024/1203. However, the approach in the description of criminal offences and the reference to multiple pieces of sectoral legislation, in terms of concepts, regulatory thresholds, etc. is no different from the previous repealed Directive. Moreover, for the interpretation and derivation of the concept of "gross negligence", reference is even made to the case-law of the Court of Justice of the European Union. In this respect, the effective transposition of the directive and the harmonization of the laws of the Member States may again not be achieved.

The clarification of some concepts, such as "ecosystem", "habitat in a protected area", "aggravating circumstances", "damage", etc. is commendable, but it is far from sufficient. In the numerous European Union acts, a number of concepts have been derived which overlap, are mutually exclusive or are relevant only to some components of the environment and not to others. For example, the notion of "disability" in the preamble to the Directive refers only to disability of persons.

A positive aspect in favor of harmonization of the Directive between Member States is the exclusion of certain forms of energy – such as heat, heat sources, noise, including underwater noise and other sources of acoustic energy, vibration, electromagnetic fields, electricity or light - among the causes of environmental harm. But again, the concept of 'energy' is derived from multiple regulations regarding different components and achieving harmonization is questionable.

The envisaged minimum and maximum limits of imprisonment for the different offences is a good approach which, if transposed effectively, would achieve the intended effect of harmonization of penalties.

3. Stronger, effective, proportionate and dissuasive penalties, alternative sanctions and measures for confiscation of the proceeds of crime

Directive (EU) 2024/1203 introduces a new, multi-layered system of sanctions for environmental crime. Central to it is the penalty of imprisonment, differentiated according to the gravity of the offence and the scale of the damage caused. This approach allows for the imposition of a fairer and more proportionate penalty, taking into account the specific circumstances of each act. The precise approach reinforces the deterrent effect, as more serious crimes are punished more severely.

The Directive takes an innovative stance by focusing not only on punishment, but also on restitution of environmental damage as ancillary sanctions and measures. These are in addition to the main penalty and include:

a) Restoration of the environment: the offender shall restore the environment to its former state as far as possible. If restoration is impossible or impracticable, financial penalties shall be imposed to compensate for the damage caused. The amount of the compensation shall be determined in accordance with the severity of the damage caused, established on the basis of expert assessments.

b) Financial penalties: The Directive provides for the imposition of fines, the amount of which is proportionate to the gravity of the offence as well as to the financial

situation of the offender. In determining the amount of the fine, factors such as the duration of the offence, the financial benefits of the criminal activity and the significance of the environmental damage caused are taken into account.

c) Additional sanctions: The Directive provides for a range of additional measures, such as disqualification from public funding (including prohibition from public procurement), revocation of permits, temporary bans on holding office, bans on standing for election, confiscation of the proceeds and proceeds of crime, etc. These measures are designed to deter future criminal activities and limit the offender's opportunities.

d) Publicity: In the public interest, the Directive allows for the publication of judicial decisions and sanctions imposed, including the personal data of convicted persons, but only in strictly justified exceptional cases to ensure a balance between the right to the protection of personal data and the public interest.

The combination of major penalties and ancillary sanctions is intended to create an effective and fair system for combating environmental crime, encouraging responsible environmental behavior and deterring future offences. In this respect, the system of sanctions envisaged is an excellent solution. The obligation to restore the environment by offenders would make a significant contribution to achieving the EU's main objective – a high level of environmental protection and improvement in the quality of the environment.

However, collateral sanctions and measures are conditional on the detection of crimes and their perpetrators and the conviction of offenders. Their implementation requires effective action by law enforcement authorities in the Member States. In this respect, the next objective is set out in the Directive.

4. *Establish a clear and effective framework for law enforcement and cross-border cooperation in the fight against environmental crim*e

Directive (EU) 2024/1203 represents a significant advance in the fight against environmental crime, especially in terms of cross-border cooperation. The emphasis on coordination between Member States and European Union agencies (Eurojust and Europol) is a positive aspect, especially given the cross-border nature of many of these crimes. Differences in national legislation as regards the means of investigation, the authorities that carry them out and the lack of trained personnel with multilayered expertise seriously hampers the investigation [8] of cross-border crime.

Effective law enforcement in relation to this type of crime requires significant resources - training of specialists, equipment of laboratories, funding of investigations, etc. The Directive does not provide specific mechanisms for securing these resources, which may make it difficult to implement in practice.

Proving environmental crime is often complex, requiring immediate and thorough expert investigative action. In many cases, specific expertise is required and evidence may be difficult to access or require expensive analysis [9]. In this respect, the introduction of effective and proportionate means of investigation, even with enhanced cooperation between Member States, is a difficult task.

For example: Investigating air pollution requires specific analyses of air samples, modeling of contaminant distribution, and identification of the source of the pollution. Cooperation with meteorological services and specialized laboratories is often necessary. The study of pollution from industrial sources, such as factories or thermal power stations, usually requires the application of sensors to measure specific pollutants such as sulphur dioxide, nitrogen oxides and fine particulate matter. In addition, a public health impact assessment is carried out. Contamination of water bodies requires water sampling at various points, identification of the contaminants, identification of the source of the contamination and assessment of the extent of the harm. All this should be done as quickly as possible and by different teams, in view of the water's ability to dissolve substances and the rapid spread of pollution. The use of specialized equipment and cooperation with hydrologists and biologists may be necessary. When investigating contamination of bodies of water, such as rivers and lakes, following incidents such as chemical accidents or spills, underwater drones and specialized equipment are often used to take samples from inaccessible locations. Analysis of aquatic plants and aquatic organisms can provide information on long-term effects on ecosystems. Illegal waste management requires verification of documentation, inspection of waste disposal sites, analysis of waste composition and identification of those responsible. Waste management experts, geologists and chemists may be needed. In cases of pesticide contamination, it is important to use specialized laboratories to measure the levels of chemicals in soil and water. This process involves agronomists and soil science experts who assess the potential risks to nature and human health. Poaching requires field work, animal tracking, DNA analysis and collaboration with foresters, conservationists and biologists.

In order to achieve effective and unified enforcement, the Directive needs to go further by developing standardized investigative methods that take into account the specificities of different types of environmental crime, the diverse forms of criminal activity, the specificities of different environmental components and the interrelationships between them.

Another positive aspect and contribution to the fight against environmental crime is the decisions on the EU-wide unification of the statute of limitations for this type of crime, which is linked to the penalty of imprisonment. Another good proposal is the possibility for Member States to provide that the statute of limitations should start to run from the moment the offence is detected, because many offences are detected at a later stage.

The decision to provide protection to persons reporting environmental crime or assisting in the investigation of such criminal activity is also positive. Granting procedural rights in environmental crime proceedings to the public concerned in the form of affected citizens, NGOs promoting environmental protection and others with an interest is also a step forward. NGOs have sufficient resources to exert public pressure on law enforcement authorities to carry out effective investigations and render fair convictions.

The introduction of a system of statistics on environmental crime and its perpetrators should also be recognized as an important step in the fight against environmental crime.

Although the many guidelines for effective enforcement throughout the EU provided for in the Directive would achieve the desired effect, more specific guidelines are needed for investigating environmental crime and proving the criminal outcome.

IV. Conclusions

Directive (EU) 2024/1203 represents a significant advance in the fight against environmental crime. It proposes an innovative and effective system of sanctions, based on a differentiated approach, with a focus on environmental restoration through accessory sanctions. By identifying real environmental threats and clearly distinguishing administrative offences from environmental crimes, the directive undoubtedly provides more effective environmental protection than the directives it repeals.

However, achieving the desired effect depends on its successful transposition by EU Member States. A weak point is the approach retained in writing out the criminal elements and the reference to the numerous acts of the Union, which is not a good approach to inferring the elements in a criminal offence.

In order to fully achieve the objectives, set out in the Directive, further action is needed to define criminal offences more clearly, with minimal reference to environmental law to derive their elements, to develop standardized methods for investigating and proving environmental damage, and to provide sufficient resources in this respect.

REFERENCES

[1] The United Nations, "World Water Development Report 2024: Water for prosperity and peace," [Online]. Available: unesdoc.unesco.org/ark:/48223/pf0000388948/PDF/388948eng.pdf.multi. [Accessed: March 27, 2025].

[2] The United Nations, "Water Development Report 2021: Valuing Water"," [Online]. Available: https://unesdoc.unesco.org/in/documentViewer.xhtml?v=2.1.196&id=p::usmarcdef_0000375724&file=/in/rest/annotationSVC/DownloadWatermarkedAttachment/attach_import_db06f7c4-b33f-4833-be56-bbf54afdee3f%3F_%3D375724eng.pdf&locale=ru&multi=true&ark=/ark:/48223/pf0000375724/PDF/375724eng.pdf#page=1&zoom=auto,-15,848. [Accessed: March 27, 2025].

[3] R. H. Cowie, P. Bouchet, and B. Fontaine, "The Sixth Mass Extinction: fact, fiction or speculation?" Biological Reviews, vol. 97, no. 2, 2017, pp. 640-663, [Online]. Available: https://doi.org/10.1111/brv.12816. [Accessed: March 27, 2025].

[4] G. Belova and G. Georgieva, "Environmental Protection as a Fundamental Human Right – The Responsibility of Local and Regional Authorities in Europe," in Proc. Environmental Challenges – Environmental and Legal Solutions, 2024, pp. 63-79, ISBN 978-954-00-0404-4.

[5] N. Krasteva and D. Atanasova, "Characterisation of Environmental Damage in Water Crime", Maritime Law and Industry, Issue 1, 2024, pp. 94-99. [Online]. Available: https://maritime.vfu.bg/arhiv.php. [Accessed: March 27, 2025].

[6] M. Faurel, "The Development of Environmental Criminal Law in the EU and its Member States," RECIEL, vol. 26, no. 2, 2017, pp. 139-146, DOI: 10.1111/reel.12204

[7] A. Nurse, "Contemporary Perspectives on Environmental Enforcement", International Journal of Offender Therapy and Comparative Criminology, 66 (4), 2022, pp. 327-344. [Online]. Available: https://doi.org/10.1177/0306624X20964037. [Accessed: March 27, 2025].

[8] E. Zębek and D. Solodov, "Environmental Forensic Examinations in Poland: a Case Study", Journal for European Environmental & Planning Law, 2021. [Online]. Available: https://brill.com/view/journals/jeep/18/1-2/article-p103_103.xml?language=en. [Accessed: March 27, 2025].

[9] K. Bobev, "Investigating Environmental Crimes, Association of Chiefs of Police Publication", Automedia BG OOD, Issue 5, 2013, pp. 18-21.

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 43-49

Identifying and Analyzing DJI Drone Signals

Vasil Andonov
NMU "Vasil Levski"
Veliko Tarnovo, Bulgaria
vasilandonov123@gmail.com

Yordan Shterev
dept. Communication and Information systems
NMU "Vasil Levski"
Veliko Tarnovo, Bulgaria
jshterev@abv.bg

***Abstract*—The widespread use of drones in commercial, industrial, military and security applications has led to a growing need for techniques to analyse their signals. Understanding the communication signals of drones is essential for applications such as airspace monitoring, counter-unmanned aerial vehicles technologies and electronic warfare. This defines the topicality of the topic. That is why the purpose of the study focuses on the identification and analysis of DJI drone signals using software defined radio. The research aims to find their frequencies usage, look for the drone activities in spectrogram, record them and characterize modulation types of drones, specifically the DJI Air 3 and Phantom 4. The working methods are based on using HackRF One software defined radio alongside the DragonOS operating system and HackRF Spectral Analyzer, SDR++ and Inspectrum software. Signal identification is performed in controlled urban and non-urban environments, allowing for the examination of telemetry signal. Different signal processing techniques are used including spectral analysis and modulation classification are applied to identify DJI drone ID. By analysing frequency bands, bandwidth requirements, and transmission structures, the study indicates how both drones communicate and adapt to environmental factors such as interference. Main conclusions from this paper are revealing that DJI drones use frequency hopping, orthogonal frequency division multiplexing modulation adapting itself with quadrature phase shift keying, 16 and 64 quadrature amplitude modulation depending on the enviroment. They also use Zadoff-Chu sequencies for synchronizing their drone ID packets. Having in mind this, the signal width and strength also chages based on the urban or no-urban environments that the drone is.**

Keywords*—DJI drones, HackRF One, signal analysis, software-defined radio.

I. Introduction

The rapid advancement of drone technology has significantly impacted various industries, including commercial and recreational applications, security, law enforcement, and military operations [1], [6]. Drones or *UAVs* are widely used for tasks such as aerial photography, infrastructure inspection, agricultural monitoring, and disaster response [15]. Understanding the signals used by drones is crucial for monitoring their activity, ensuring regulatory compliance, and developing counter-drone strategies, when necessary [2], [8]. This defines the topicality of the topic.

DJI is one of the leading manufacturers of consumer and professional drones [4]. They use advanced wireless communication protocols to maintain stable control links and transmit telemetry data in real time [9], [11], [16]. These transmissions include essential information such as GPS coordinates, altitude, speed, battery levels, and other flight parameters [3], [13]. Analysing these signals can provide valuable insights of drone behaviour, operational patterns, and potential vulnerabilities. However, as drone communication protocols evolve, they become more secure by using encryption and frequency-hopping techniques, which make signal interception and analysis more complex [2], [8].

In [3], [8], [16] experiments are focused more on analysing drone communication protocols and their structures. Comparing to this paper, it is shown more practically visualisation of their signals.

SDRs are powerful tools for analysing drone signals due to their ability to capture a wide range of frequencies. Devices like the *HackRF One*, combined with operating systems such as *DragonOS*, allow to identify transmission characteristics, and classify different types of drone signals based on their frequency bands, modulation schemes, and bandwidth usage [10], [14], [19].

The purpose of the study aims to discuss the methodology applied in this research for spectrum analysis, pattern recognition, and frequency monitoring, providing a systematic approach to examining drone communication signals.

II. Materials and Methods

To effectively analyse *DJI drone signals*, a combination of hardware and software tools are used. The

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8486
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

primary hardware used in this study was the *HackRF One* on *Fig. 1*. It is a versatile *SDR* capable of transmitting and receiving signals within a wide frequency range *(1MHz to 6GHz)*. This device was selected due to its affordability, open-source nature, and compatibility with multiple *SDR* software tools. *HackRF One* provides real-time access to the electromagnetic spectrum, allowing to capture and analyse drone transmissions.

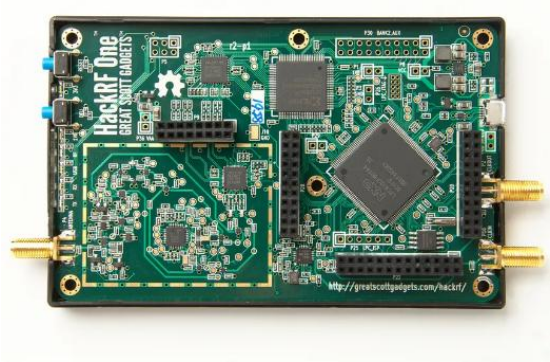


Fig. 1. HackRF One Board.

The *DragonOS* is Linux distribution. It was used as the operating environment for the *SDR-based* signal analysis. *DragonOS* is a pre-configured operating system that includes various open-source *SDR* tools. This is making it an ideal choice for researchers analysing wireless communications. It includes softwares for recording, processing and visualizing captured or live signals.

HackRF Spectrum Analyzer is a real-time spectrum monitoring software, is used to find drone activities and also to see a drone signal look like. After that a *DJI drone ID* with *SDR++ have been recorded.* Finally, with the help of *Inspectrum* software analyze the actual modulation characteristics.

A. Signal identification and visualization

DJI Air 3 and *Phantom 4* use *OcuSync* or *Lightbridge* radio protocols. OcuSync is used in *DJI drones* for transmitting video and control signals. It is part of the *Lightbridge* family and is designed to offer low-latency HD wireless video and control signals, allowing long-range transmission. OcuSync supports dual-frequency bands of *2.4 GHz* and *5.8GHz*, which gives it more flexibility in areas with interference [1], [3]. It can automatically switch between these frequencies to maintain a stable connection. It has a range of up to *4.3 miles (7 km)* and can transmit video at *1080p* resolution. On the other hand, *Lightbridge* is an older protocol with the same range but with a lower video resolution of *720p*.

Both radio protocols use *Orthogonal Frequency Division Multiplexing (OFDM)* modulation. This is a transmission technique that divides a data stream into multiple smaller subchannels, as you can see on *Fig. 2*, each carrying part of the information across closely spaced frequencies, rather than using a single wideband channel [9]. Unlike traditional single-channel modulation, where data bits are transmitted sequentially, *OFDM* allows multiple bits to be sent simultaneously across parallel subchannels. This reduces the required data rate per subchannel, making the system more resistant to interference and improving spectral efficiency [1]. While primarily used in wireless communication, *OFDM* is also applied in wired and fiber optic networks for reliable high-speed data transmission.

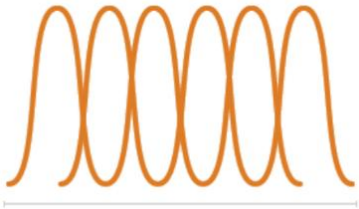


Fig. 2. OFDM subchannels overlapping.

Lightbridge is used in older *DJI* models like the *Phantom 4*, leverages *OFDM* to maintain stable video and telemetry transmission over extended distances. *OcuSync* is an evolution of *Lightbridge*, further optimizes *OFDM* by incorporating adaptive frequency hopping, improved error correction, and dynamic bandwidth allocation, allowing it to switch between *2.4GHz* and *5.8GHz* for better interference avoidance [3]. These enhancements make *OcuSync* more robust in complex *RF* environments, providing lower latency, higher data rates, and increased range compared to traditional single-carrier transmission methods.

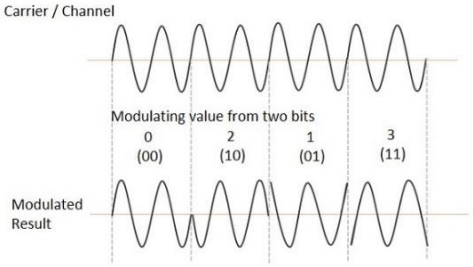


Fig. 3. QPSK waveform.

In the other hand, based on signal quality within *OFDM*, subcarriers use different modulation schemes. They are *Quadrature phase-shift keying (QPSK), 16 and 64 Quadrature amplitude modulation (QAM)*. *QPSK* is a modulation technique that allows the transmission of multiple bits simultaneously by representing possible states with different analog levels and phases *(Fig. 3)* [10]. It improves spectral efficiency by transmitting two bits using the same spectrum width as *Binary Phase Shift Keying (BPSK)*, with the *I (in phase)* and *Q (quadrature)* channels modulated onto carriers *90°* apart [7]. Both drones, *DJI Air 3* that uses *OcuSync 4.0* and *DJI Phantom 4* working with *Lightbridge* rely on *QPSK* to establish stable, long-range, and interference-resistant links between drones and controllers.

In *16-QAM*, each symbol is represented by *4 bits* of data, allowing for *16 different states*, while in *64-QAM*, each symbol is represented by *6 bits* of data, allowing for *64 different states* - *Fig. 4* [12]. The main difference between *16-QAM* and *64-QAM* lies in the number of bits

per symbol and the number of states they can represent. *16-QAM* has *16* possible states, whereas *64-QAM* has *64* possible states [5]. This means that *64-QAM* can transmit more data per symbol than *16-QAM*, but it is also more susceptible to noise and interference, making it less robust in low *Signal-to-Noise Ratio (SNR)* conditions [18].



Fig. 4. 16 and 64 QAM constellation.

By combining *OFDM's* multi-carrier transmission with adaptive modulation, *DJI's Lightbridge* and *OcuSync* achieve low-latency, high-quality video streaming and robust control links. In strong signal conditions, *64-QAM* maximizes data throughput, while in weaker or noisier environments, the system can downgrade to *QPSK* to maintain a stable connection.

B. Recording a DJI drone ID

DJI drone ID is the identification system used by *DJI* drones to provide information about the drone and its operator [13]. This system is designed to comply with the Remote ID requirements set by the *Federal Aviation Administration (FAA)* and other regulatory people around the world. Remote ID allows drones to transmit identification and location data to other parties, enhancing safety and security in the airspace [1], [4]. *DJI* drones can use various methods to transmit this information, including Wi-Fi, Bluetooth, or cellular networks, depending on the model and the specific Remote ID requirements in their operating region. Center frequencies depend on the band that is used [3]. In *table 1* there are shown *2.4GHz* and *5.8GHz* bands.

SDR++ is an open-source, cross-platform *SDR* receiver application. It provides a powerful and flexible interface for tuning, demodulating, and analyzing radio signals from various SDR devices, including *HackRF One*. Using this software, *drone ID* can be recorded by selecting one of the center frequencies listed above. The recording file format needs to be *float32*. It is a *32-bit* floating-point format used in computer memory to represent a wide dynamic range of numeric values by using a floating radix point [17]. *Float32* is preferred due to its higher precision and dynamic range. This is crucial for capturing weak or noisy signals. *Float32* minimizes quantization errors, preserving fine details essential for accurate demodulation, especially for signals using *OFDM* or frequency hopping.

SDR++ is an open-source, cross-platform *SDR* receiver application. It provides a powerful and flexible interface for tuning, demodulating, and analyzing radio signals from various SDR devices, including *HackRF One*. Using this software, *drone ID* can be recorded by selecting one of the center frequencies listed above. The recording file format needs to be *float32*. It is a *32-bit* floating-point format used in computer memory to represent a wide dynamic range of numeric values by using a floating radix point [17]. *Float32* is preferred due to its higher precision and dynamic range. This is crucial for capturing weak or noisy signals. *Float32* minimizes quantization errors, preserving fine details essential for accurate demodulation, especially for signals using *OFDM* or frequency hopping.

TABLE 1 DJI DRONE ID CENTRE FREQUENCIES

Frequency Bands	
2.4GHz	**5.8GHz**
2399.5MHz	5741.5MHz
2414.5MHz	5756.5MHz
2429.5MHz	5771.5MHz
2444.5MHz	5786.5MHz
2459.5MHz	5801.5MHz
	5816.5MHz

C. Analyzing DJI drone ID packet

One of the main characteristics of a *drone ID* is the *Zadoff-Chu (ZC) sequence*. It is a special mathematical sequence used in transmissions for synchronization and signal detection. It has key properties like constant amplitude and zero cross-correlation, making it highly effective for timing alignment and interference resistance in wireless communication [19]. In *DJI* drones, the *ZC sequence* helps receivers accurately detect and decode *Drone ID* signals, even in environments with *RF* noise and interference [11], [13].

The *ZC sequence* enhances signal accuracy by reducing timing errors and improving synchronization. It minimizes interference and distortion, ensuring clear and reliable transmission [19]. Each *Drone ID* transmission consists of nine *OFDM* symbols, with the *ZC sequence* embedded in symbols *4* and *6* [3], [16]. These special symbols act as reference points, allowing the receiver to synchronize with the transmission. The remaining symbols contain identification and telemetry data, such as the drone's serial number, GPS position, and flight status.

III. RESULTS AND DISCUSSION

On *Fig. 5* is the experimental setup. There are both drones, on the left is *DJI Air 3* with the controller and on the right is *DJI Phantom 4* again with his controller. *HackRF One* works with a tri-band antenna, and it is connected to a laptop with *DragonOS* operating system.

A. Identifying drone signals

Based on the methodology, first experiment is identifying a drone signal in urban and non-urban environment. It is used a tri-band *(GSM, 4G and 5G)* antenna with frequency range from *600MHz* to *6GHz* connected to *HackRF One* working with *HackRF Spectre*

Analyzer software on *DragonOS*. At the beginning on *Fig. 6* and *Fig. 7* are the spectrograms in urban and non-urban environment with the *DJI Air 3* powered off. The frequency range is set to be *2300MHz–2600MHz* to have clear view of *2.4GHz* band.



Fig. 5. Experimental setup softwares and hardwares.

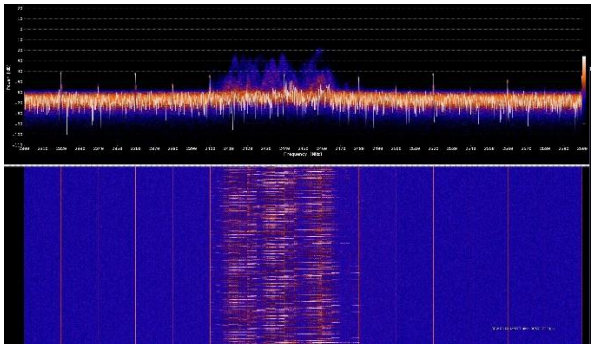


Fig. 6. The Spectrogram in urban environment with drone powered off. Power levels from -75dB to -50dB with PSD frequency range from 2405MHz to 2465MHz.

On *Fig. 6* the spectrogram has only short bursts that indicate the usage of *Wi-Fi*, *Bluetooth* and smart home devices. This is because the experiment is in an urban environment. After that on *Fig.7* is the same test but in non-urban environment. The differences are quite big. The spectrogram is much clearer because of there are fewer *Wi-Fi* routers, cellular towers, or other strong *RF* emitters in the *2.4GHz industrial, scientific and medical (ISM)* band. The few narrowband spikes are from distant sources, background noise, or minor reflections.

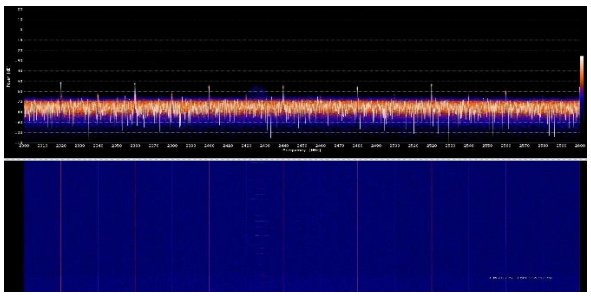


Fig. 7. The spectrogram in non-urban environment with drone powered off. Power levels from -100dB to -70dB with no frequency usage.

Then on *Fig. 8* and *Fig. 9* are the spectrograms with the drone powered on. The *RF* spectrum changed significantly due to the introduction of multiple wireless transmissions. Before the drone is powered on, the baseline spectrogram primarily shows background *RF* noise and interference from nearby *Wi-Fi*, *Bluetooth*, and other *ISM-band* devices. The signal power levels remain relatively low between *-100dB* and *-50dB*.

However, when the drone is powered on, it immediately begins broadcasting signals, which results in a higher *power spectral density (PSD)* in frequency range from *2360MHz* to *2500MHz* in urban environment *(Fig. 8)* and in non-urban environment from *2435MHz* to *2470MHz (Fig. 9)* with power levels reaching *-18dB*.

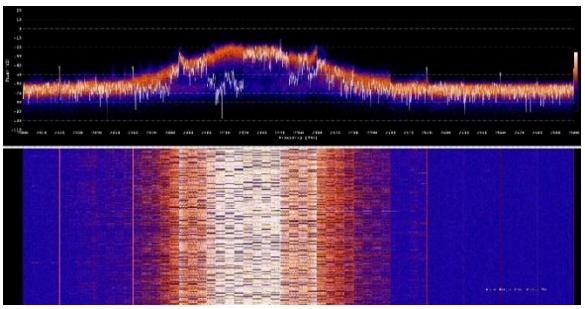


Fig. 8. The spectrogram in urban environment with DJI Air 3 powered on. Power levels from -70dB to -18dB with PSD frequency range from 2360MHz to 2500MHz.

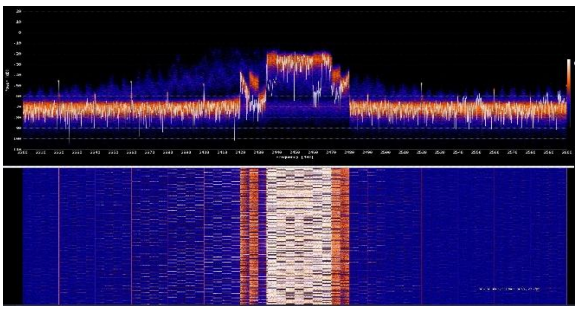


Fig. 9. The spectrogram in non-urban environment with DJI Air 3 powered on. Power levels from -75dB to -20dB and PSD frequency range from 2435MHz to 2470MHz.

The spectrum analyzer also displays wide, consistent, repeating signal bursts, suggesting for frequency hopping methods in *OFDM* modulation. The drone adapts by dynamically adjusting its power levels and switching channels frequently in an attempt to maintain a stable connection. The hopping behavior is more structured and predictable in non-urban environments as can be seen on *Fig. 9* but becomes more irregular and adaptive in urban environments where interference levels are higher, *Fig. 8*.

Comparing the *DJI Phantom 4* signals to the *Air 3* ones the differences are visually big - *Fig.10*. Phantom *4's* signal appears more structured and concentrated within a specific range from *2415MHz* to *2425MHz*. This is because this drone uses the Lightbridge radio protocol which is not so adaptive as OcuSync used in DJI Air 3. It has strong, periodic peaks in the waterfall display, meaning it follows a fixed frequency hopping pattern rather than dynamically adjusting its transmission as *Air 3* on *Fig. 8*.

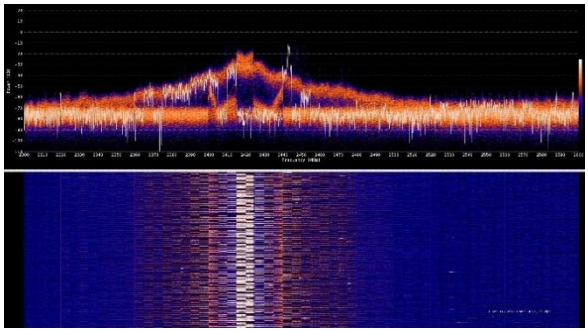


Fig. 10. The spectrogram in urban environment with DJI Phantom 4 powered on. Power levels from -90dB to -18dB with PSD frequency range from 2400MHz to 2440MHz.

Overall, the *Phantom 4* uses an effective but less adaptive communication system compared to the *Air 3*, which employs a wider and more interference-resistant transmission method. The *Air 3's* spectrum characteristics make it better suited for urban conditions with high *RF* congestion, while the *Phantom 4* may function more reliably in less crowded *RF* environments, where fixed frequency hopping patterns are less likely to be disrupted by external interference sources.

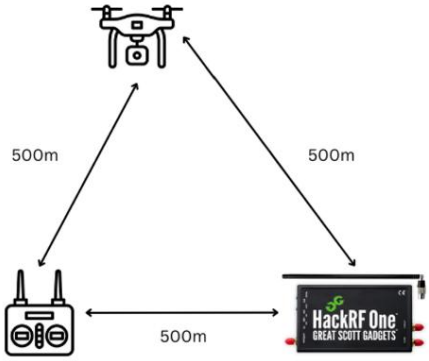


Fig. 11. Real-life scenario of detecting a drone.

The next experiment is a more real-life scenario of detecting a drone signal in big distances. On *Fig. 11* is an illustration of the experimental setup. The drone controller is *500m* from *HackRF One*. The drone is *500m* hight and *500m* from *HackRF* too.

The spectrogram on *Fig. 12* shows the usage of a drone around. The *PSD* is from *2435MHz* to *2470MHz,* and the power levels are reaching *-50dB*. The signals are not so strong but because there are repeating signal bursts and frequency hopping can say that these are drone signals. By this experiment it can be said that *HackRF* can be used also as a drone detector on a not so small distance in real-life implementations.

B. Recording a DJI drone ID packet

The next experiment is recording a drone ID using again *HackRF One*, *the tri-band antenna* and *SDR++* software on *DragonOS*.

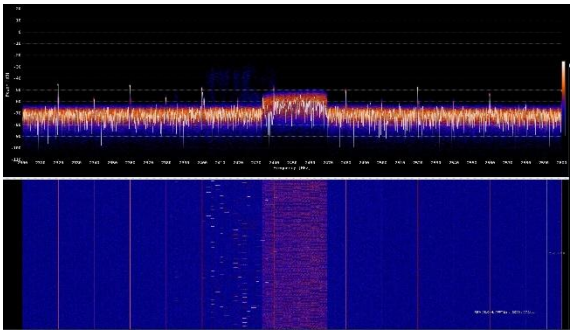


Fig. 12. The spectrogram of the real-life scenario experiment. Power levels from -80dB to -55dB with PSD frequency range from 2435MHz to 2470MHz.

Having in mind the center frequencies of *drone ID* in *table 1* one of them is set and make a *float32* record. In the example it is used *2444.5Mhz - Fig. 13* and the duration of the recording is *10 seconds*. *DJI drone ID* is transmitted *10 times per second* and the adaptation of frequency that is used on because of frequency hopping adjustments. That is why a *10sec.* recording is enough for the experiment.

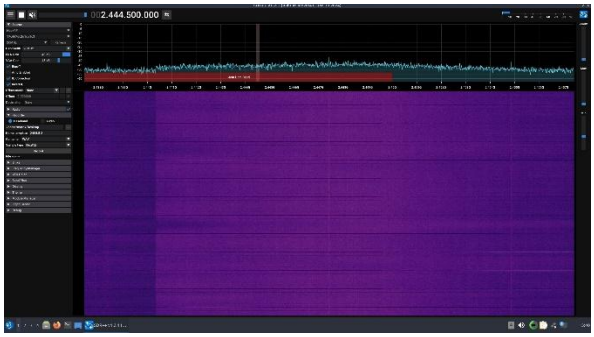


Fig. 13. SDR++ recording a DJI drone ID on 2444.5MHz center frequency.

This can be done with every of the frequency shown in *table 1*. Transition of *drone ID* depends on the environment that you are in. In non-urban environments, *ID* transmission remains stable with minimal interference but in urban environments, signal congestion and multipath effects can cause packet loss or frequency hopping adjustments, leading to slight variations in transmission timing and frequency usage.

It has been observed that even when a user manually sets the *DJI OcuSync* downlink to operate strictly within the *2.4GHz* or *5.8GHz* range, the *DJI drone ID* signal does not conform to these settings and continues transmitting on the frequencies in *table 1* [3].

A. Analyzing a DJI drone ID

Finally, when the recording of center frequencies listed in *table 1* is made, open it in *Inspectrum* on *DragonOS* to analyze the specter deeply. In our example the recording of 2.444.5MHz frequency is used.

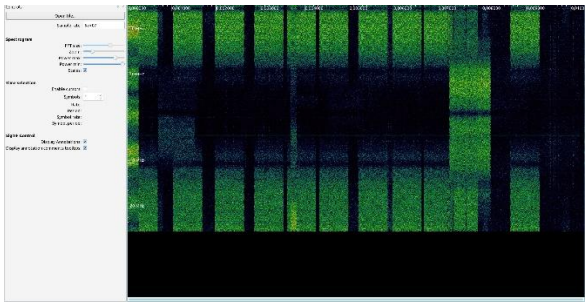


Fig. 14. Analysis of drone IDs on Inspectrum software.

The spectrogram on *Fig. 14* captures *RF* signals over time and shows their frequency characteristics. The sample rate of *5e+07 (or 50 MHz)* is used to capture signals at a high enough resolution to analyze the details of *RF* transmissions. The frequency range spans from *0MHz* to *20MHz*, as indicated by the *Y-axis*, with signal bursts appearing throughout this range. These bursts, separated by quiet periods, are characteristic of the *Drone-ID RF* frame structure. This pattern is consistent with the expected behavior of a communication system used for *Remote ID*, where data packets are transmitted in structured bursts at regular intervals.

The time window captured by the spectrogram spans about *10 milliseconds*. Each vertical group of lines in the spectrogram corresponds to one of these signal bursts, suggesting that each burst represents a packet of data being transmitted at specific intervals. Each frame's bandwidth range from *9.38MHz* to *10.91MHz*. In the spectrogram, the signal shifting slightly across the frequency domain, which corresponds to the *CFO* variations in the packet analysis. These shifts are visible as slight changes in the positioning of the bursts on the frequency axis. The regular pattern of bursts observed also in the spectrogram in *Fig. 14* suggests the usage of *Zadoff-Chu (ZC)* sequences. These bursts occur at precise intervals, which is typical of systems using *ZC sequences* to maintain synchronization.

IV. Conclusion

The methodology applied in this research integrates spectrum analysis, pattern recognition, and frequency monitoring, providing a systematic approach to examining drone communication signals. By SDR technology like HackRF One with tools such as HackRF Spectrum Analyzer, SDR++ and Inspectrum, it was capture, visualize, and analyze the behaviour of DJI Air 3 and Phantom 4 signals across urban and non-urban environments. Also, it is demonstrated capabilities of the methodology that reach up to 500m drone signal detection. Theoretically, the ability to study drone signals at the raw RF level allows for a detailed examination of frequency utilization, modulation schemes, bandwidth variations, and transmission stability.

Spectrum analysis plays a critical role in identifying occupied frequency bands, signal strength variations, and interference levels. By monitoring the 2.4GHz band, it is determined which frequencies are used for telemetry data, as it shown in table 1. The application of spectrogram visualization enables researchers to track signal evolution over time, revealing patterns such as frequency hopping, channel allocation, and power adjustments in response to environmental conditions.

Pattern recognition techniques help distinguish recurring structures in drone transmissions, allowing to differentiate between control commands, telemetry bursts, and video signals. It is discovered that each DJI Remote ID bandwidth ranges from 9.38MHz to 10.91MHz with precise intervals, which is typical of systems using ZC sequences to maintain synchronization. The identification of repeated frequency hopping intervals and unique transmission signatures provides deeper insight into how DJI drones maintain stable communication links

Practically, findings of this study significantly contribute to counter-drone measures, regulatory enforcement, and spectrum management. Understanding the characteristics of UAV communications enables researchers, security professionals, and regulatory agencies to develop effective detection and mitigation strategies. For instance, identifying distinct frequency hopping patterns and modulation schemes allows the creation of automated drone detection systems, which can track UAV activity based on its unique RF footprint. Future research could focus on analysing 5.8GHz signal characteristics, evaluating long-range signal propagation, and investigating encryption methods within DJI transmissions. Expanding these studies will further enhance ability to detect, monitor, and regulate drone activity in both civilian and military applications.

Acknowledgments:

This report is supported by the National Scientific Program "Security and Defence", approved by Decision No. 171/21.10.2021 of the Council of Ministers of the Republic of Bulgaria.

REFERENCES

[1] D. Aouladhadj, E. Kpre, V. Deniau, A. Kharchouf, C. Gransart, C. Gaquière, "Drone Detection and Tracking Using RF Identification Signals", Sensors, 2023, 23, 7650. https://doi.org/10.3390/s23177650.

[2] A. Bello, Radio Frequency Toolbox for Drone Detection and Classification. Master of Science (MS), Thesis, Electrical & Computer Engineering, Old Dominion University, 2019. DOI: 10.25777/9gkmjd54. Available: https://digitalcommons.odu.edu/ece_etds/160. [Accessed Feb. 23, 2025].

[3] C. Bender, DJI Drone IDs Are Not Encrypted. *arXiv*, 2022. https://doi.org/10.48550/arXiv.2207.10795.

[4] D. Clark, C. Meffert, I. Baggili, F. Breitinger, DROP (DRone Open Source Parser) Your Drone: Forensic Analysis of the DJI Phantom III. *Digital Investigation* 2017, 22, S3-S14. https://doi.org/10.1016/j.diin.2017.06.013.

[5] Constellation Diagram. *Wikipedia*. Available: https://en.wikipedia.org/wiki/Constellation_diagram. [Accessed Feb. 23, 2025].

[6] DJI Drone Operators' Location Intercepted. *DroneXL*, 2 March 2023. Available: https://dronexl.co/2023/03/02/dji-drone-operators-location-intercepted/. [Accessed Feb. 23, 2025].

[7] Digital Communication: Quadrature Phase Shift Keying. TutorialsPoint. Available: https://www.tutorialspoint.com/digital_communication/digital_communication_quadrature_phase_shift_keying.htm. [Accessed Feb. 23, 2025].

[8] Master Thesis on DJI Protocol Reverse Engineering. Digidow, Available: https://www.digidow.eu/publications/2021-christof-masterthesis/Christof_2021_MasterThesis_DJIProtocolReverseEngineering.pdf. [Accessed Feb. 23, 2025].

[9] Orthogonal Frequency Division Multiplexing. TechTarget. Available: https://www.techtarget.com/searchnetworking/definition/orthogonal-frequency-division-multiplexing. [Accessed Feb. 23, 2025].

[10] Phase Shift Keying: Implementation. Wikipedia. Available: https://en.wikipedia.org/wiki/Phase-shift_keying#Implementation_2. [Accessed Feb. 23, 2025].

[11] Phase Shifting Techniques in Communication. *arXiv*, 2022. Available: https://arxiv.org/abs/2211.05702. [Accessed Feb. 23, 2025].

[12] Quadrature Amplitude Modulation. Wikipedia. Available: https://en.wikipedia.org/wiki/Quadrature_amplitude_modulation. [Accessed Feb. 23, 2025].

[13] Research Square: RF Toolbox for Drone Detection. Available: https://assets-eu.researchsquare.com/files/rs-5827543/v1_covered_58ee4e7b-b0e4-4d34-b0d9-4d5fbac723d7.pdf. [Accessed Feb. 23, 2025].

[14] RTL-SDR: Drones. Available: https://www.rtl-sdr.com/tag/drone/. [Accessed Feb. 23, 2025].

[15] S. Kreps, Drones: What Everyone Needs to Know, ISBN 978–0–19–023535–2, Oxford University Press 2016.

[16] N.Schiller, M. Chlosta, M. Schloegel, N.Bars, T. Eisenhofer, T. Scharnowski, L. Schönherr, T. Holz, Drone Security and the Mysterious Case of DJI's DroneID. ISBN 1-891562-83-5, 3 March 2023. Available: https://dx.doi.org/10.14722/ndss.2023.24217.

[17] Single-Precision Floating-Point Format. *Wikipedia*. Available: https://en.wikipedia.org/wiki/Single-precision_floating-point_format. [Accessed Feb. 23, 2025].

[18] Types of Quadrature Amplitude Modulation. Electronics *Notes*. Available: https://www.electronics-notes.com/articles/radio/modulation/quadrature-amplitude-modulation-types-8qam-16qam-32qam-64qam-128qam-256qam.php. [Accessed Feb. 23, 2025].

[19] Zadoff–Chu Sequence. Wikipedia. Available: https://en.wikipedia.org/wiki/Zadoff%E2%80%93Chu_sequence#cite_note-Zepernick-1. [Accessed Feb. 23, 2025].

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 51-56

Digital Technological and Legal Support of the Illegal Migration Control: a Population and National Security Aspects

Ilona Bulgakova
Economic and Management center
Riga Technical University Rezekne Academy
Rezekne, Latvia
ilona.bulgakova@rta.lv
bulgakova@inbox.lv

Artūrs Gaveika
Economic and Management center
Riga Technical University Rezekne Academy
Rezekne, Latvia
arturs.gaveika@rta.lv
argavs@inbox.lv

Ilga Krampuža
Economic and Management center
Riga Technical University Rezekne Academy
Rezekne, Latvia
ilga.krampuza@rta.lv
ahia@rta.lv

***Abstract*—Control over the problem of illegal migration as a subsector of migration in the Republic of Latvia is one of the tasks to be implemented by the executive power, such as the Ministry of the Interior and its subordinate institutions, mainly the State Border Guard and the Office of Citizenship and Migration Affairs. The purpose of the article is to study digital technological and legal solutions for controlling illegal migration through the prism of population and national security. The following research methods were used in the development of the study: descriptive, analytical, statistical analysis, inductive method. Results of the study: 1) the regulation of identified digital technological security (tools and means) of illegal migration and problems related thereto, in the context of the position of the State of Latvia in control of illegal migration; 2) the official statistics of illegal migration (data of the State Border Guard of the Ministry of Interior and the Office of Citizenship and Migration Affairs) (statistical data on criminal and administrative offenses) were compiled for the last three-year period, taking into account also latent illegal migration approximate indicators; 3) problems identified in the application of the digital, technical and legal regulation of illegal migration in the State border and within the State, which officials encounter in the practice of law enforcement.**

***Keywords*— digital technical security, illegal migration and its control, legal security, national security**.

I. INTRODUCTION

At the level of EU policy priorities, the Stockholm Program outlined several aspects, starting with the protection of individuals' fundamental rights and freedoms within the so-called personal security paradigm, European rights and justice, the protection of the European area, and Europe's responsible role in the world (aspects of European freedom, security, and justice) [1].

Several security paradigms are described in literature sources. The traditional security paradigm prioritizes national and state security, whereas the personal security paradigm considers the individual as the primary object to be protected. The social security paradigm positions society as the central object of security threats. For a long time, the European strategy in the field of social protection was based on the personal security doctrine. However, given the significant increase in the degree of social security threats, it became necessary to focus on the understanding of so-called "initial" security, whose main goal is to protect the public sphere, allowing the implementation of secret and non-transparent security and surveillance measures, justified by so-called "emergency" measures [e.g., 2].

From a socio-economic aspect, in the context of the security of the EU's external borders, there are several groups of risks and levels. From the perspective of the residents living near the Latvian border, as well as the legal perspective, one of the sociological studies (2021) emphasized that in some of the regional municipalities in Latvia there is a lack of reflection of public security aspects in policy planning documents or their specifically outlined results (e.g., Rezekne's territorial planning for 2018-2030, the situation as of 2021). Within the vision of the "Rezekne City Sustainable Development Strategy 2030," the task of "building Rezekne as a human and environmentally friendly, safe, and modern city on the eastern border of the European Union" is mentioned. Indirectly, threats to the public security sector are defined in relation to improving the quality of education, preserving cultural and ethnic

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8498
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

diversity, and strengthening social integration.. According to the SWOT (SWOT – strengths, weaknesses, opportunities, threats) analysis, potential threats include a lack of connection between different planning levels and an insufficient number of attendees at cultural events (therefore, we can see the problem of diminishing affiliation with Latvian culture) [3].

The topicality of the study is determined by the global and regional challenges of recent years, which involve not only migration, but also illegal migration problems in Latvia as an EU Member State. Along with significant changes at the international level, improvements are also needed in the area of prevention and measures to combat illegal migration. And taking into account that the task of preventing illegal migration in Latvia is implemented by the State institution, i.e. the State Border Guard, these improvements are a topical matter exactly in the activities of this institution mentioned above, as well as in the activities of other State institutions that support the State Border Guard and cooperate with it in the field of prevention of illegal migration.

Consequences of illegal migration. These consequences occurs both for illegal migrants themselves and for the state. From a human rights perspective, illegal migrants are exposed to risks of exploitation and human trafficking. For example, one of the latest cases of a human trafficking network being uncovered and dismantled is the one reported by the Spanish police at the end of February 2025, who arrested 48 people in connection with the sexual exploitation and forced labour of more than 1,000 women, mainly from Colombia and Venezuela) [4].

The end of the 20th century and the 21st century are the era of high technology, offering various identification options exist. In this era of high technology, accurate identification is of crucial importance because it guarantees security and reliability. Every system or process uses trusted identification to ensure that only verified users are given access [5].

In an anterview, the Minister of the interior R. Kozlovskis expressed the oponion: Smart borders are modern border control systems that use automated technologies to manage the flow of persons and vehicles between countries efficiently, safely and quickly. Unlike traditional borders in recent history, where checks were largely manual, smart borders are based on modern solutions [6].

Future challenges could be related to the ever-increasing number of travelers, increasingly complex threats, and possible hybrid threats from individual countries. Undeniably, this will require new, innovative approaches to border control and immigration control within countries. Smart borders help to mitigate security risks, as there is still a possibility of entering the EU or Schengen area countries with criminal intentions, creating potential security risks in the future [7].

The fourth section of the Schengen Convention, the Schengen Information System (SIS), is of great importance in the work of law enforcement agencies. It provides for a global information system for combating crime and cooperation between Member States and is in force in most EU countries and the Schengen associated countries of Switzerland, Norway, Liechtenstein, and Iceland. Every day, around 3.5 million people cross internal borders for work or study or to visit families and friends, and almost 1.7 million people reside in one Schengen country while working in another [8].

The use of the SIS has led to significant changes in the regulation of the immigration process in each Schengen Member State [9].

The purpose of this is to strengthen public policy and public security on the territory of the Member States by ensuring the availability of reports to the competent authorities and institutions of the Member States (Schengen Information System Operating Law, 2007) [10], although these reports sometimes do not contain sufficient grounds of public policy interests to refuse entry to individuals [11].

Key smart border IT (information technology) tools are constantly being improved to help combat crime and protect national borders: Visa Information System (VIS) (Schengen Visa info, 2023), Entry/Exit System (EES) (Regulation (EU) 2017/2226 (Regulation EU 2017), European Travel Information and Authorization System [12].

The Criminal Law also contains provisions on liability for illegal crossing of the state border (Criminal Law, Article 284), ensuring the possibility to illegally reside in the Republic of Latvia (Criminal Law, Article 285 prim), as well as ensuring in bad faith to a person the possibility to acquire the legal right to reside in Latvia, another Member State of the EU, a country of the EEA (European Economic Area) or the Swiss Confederation (Criminal Law, Article 285^2) [13].

II. MATERIALS AND METHODS

Article 4 of the State Border Guard Law defines the main functions of the Border Guard, namely ensuring the inviolability of the State Border and preventing illegal migration. The implementation of the above tasks should extend not only to the activities of the border protection itself, but also to activities within the state, thereby ensuring the security of the population and national security in general. The use of criminal and administrative legal means to control illegal migration is also the responsibility of other competent bodies, such as the State Police, which is subordinate to the Ministry of Internal Affairs. In particular, the challenges of recent years in the field of illegal migration on the state border and within the Republic of Latvia make this issue even more important and urgent.

The research hypothesis is defined as follows: in the field of illegal migration, new challenges are emerging, the prevention and control of which requires technical and legal solutions that meet the requirements of modern technological and public relations development. The object

of the study is the legal relations in the field of control over illegal migration. The subject of the study is the possibilities of digital technological and legal security for controlling illegal migration in the application of legal relations.

The following research methods are used in the development of the study: a) descriptive (describing the problem of illegal migration and its impact on society as a whole, on legal relations based on the situation in Latvia), b) statistical analysis method (by analysing the number of cases detected in criminal offences directly related to illegal migration (illegal crossing of the State border and unlawful conveyance of a person Across the State Border) for the last 10 years, i.e., in the period from 2014 to 2024), c) analytical method (performing analysis of changes in the potential threat of illegal migration from the point of view of criminological forecasting), as well as sociological observation method (authors of the article, applying personal professional experience, legal practices in the field of administrative and criminal law, as well as institutions responsible for the prevention of illegal migration, i.e. in the field of activity of the State Border Guard).

III. RESULTS AND DISCUSSION

Situations/types of illegal migration (based on the example of illegal crossing of the state border). There are several situations that illegal/potential illegal migrants find themselves in. The above situations can be divided into the following groups: a) a person/group of persons crosses the state border through the border control points without a visa with a valid/invalid/forged document for travel or without valid travel documents or without any documents that could identify the person; b) a person/group of persons crosses the state border through the "green border" (outside the territories of border control points) and is detained on the so-called "green border". They could also be *potential victims of human trafficking,* beginning with carriers (including in practice as carriers or so-called "wearers", among whom in practice there were citizens of other countries, as well as local residents living in the border area who are looking for means of subsistence, or residents who do not have a legal income, with a low income level, with an insufficient standards of living, and who their own personal motivation), and ending wanted for committing crimes; c) a person or persons who cross the state border outside the border control points (bypassing the established procedure) through the "green border" as unidentifiable and are illegally staying in the country.

A. Digital technical solutions for combating illegal migration

The legal framework of the European Union includes Regulation (EU) 2016/399 [14], or the Schengen Borders Code, which is directly linked to the so-called Smart borders. The above Regulation establishes the rules and procedures for border crossings at both the internal and external borders of the EU. Smart borders are an important tool that helps Member States effectively implement the principles of border control, ensuring both security and efficient management of persons and their flows.

Automated document scanners with biometric data [15] (face, fingerprints, fingermarks and palmmarks, DNA (for missing or wanted persons) reading capabilities have been implemented in SIS since March 2023 [16]. These modern technologies, as an integral part of the smart border, are especially important at control points with a large simultaneous flows of people, in such places as airports, ports and railway stations at state borders, but also at border crossing points on roads, where the flow of people is more uniform, the use of such modern technological tools would be necessary to avoid queues and conduct border control as quickly as possible, reduce the number of errors and help border crossing persons navigate the border control procedure. Opinions and insights about this have already been expressed in the literature [e.g.,17].

Artificial intelligence also plays a significant role in the operation of the smart border, processing in real time [18] not only biometric, but also other data, such as information obtained about vehicles, including their number plates and other information [19].

The digitalization of personal data and the increasingly active use of technical and digital means for obtaining biometric data contribute to the protection of human rights and also have a positive impact on the control of illegal migration. Another challenge is the ability of smart devices to operate in various weather conditions, in conditions of limited communication and electricity, along with work organization issues, lack of human resources and finances, issues of normative framework, and high costs for both acquiring and maintaining the technology.

In 2024, at the 9th International Scientific and Practical Conference "Border Security and Management", representatives of Latvia, neighbouring countries and other Schengen countries, based on risk analysis, survey data and other performance indicators, as well as institutional reports, identified the main problems of the implementation and operation of smart borders, including the lack of regulation at both the EU and national levels, problems with the principle of solidarity in the EU and Schengen countries, the operability of smart devices, and high costs of acquiring and maintaining technologies [20]:

- high costs of both acquiring and maintaining technology;
- limited interoperability of systems and system management problems, sometimes linked to staff management problems and their turnover;
- lack of human and financial resources.

B. Legal solutions to prevent illegal migration

From a human rights perspective, becoming an illegal migrant can occur due to different circumstances beyond person's control (global or regional events) and/or due to events in a person's life. Illegal migrants are exposed to

high risks of various forms of exploitation. Illegal migration, on the other hand, as a negative phenomenon, also poses a threat to the state as well as to the security and public order of the designated territories, and public safety. Because of illegal status, illegal migrants are denied the opportunity to legally earn a living, pay taxes, obtain an identity document, as well as residence permits in the relevant EU member state.

There are various legal tools to prevent and control the problem of illegal migration. And such tools could be divided into several groups. Figure 1 illustrates the legal solutions to prevent illegal migration. *Figure 1 clearly illustrates the legal means of preventing illegal migration (the authors this article developed).*

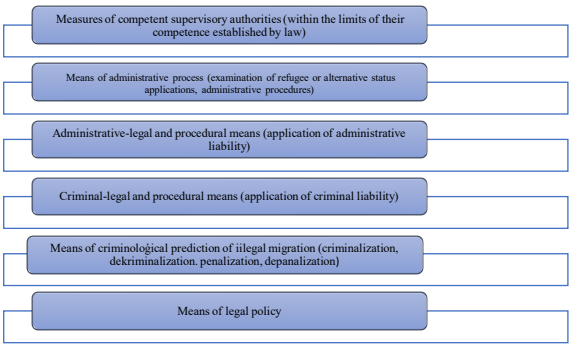


Fig.1. *Legal means to prevent illegal migration*

Figure 1 shows four types of groups of legal measures to prevent illegal immigration. The first group includes measures taken by competent and responsible authorities to prevent illegal immigration. Article 4 of the State Border Guard Law includes the task of preventing illegal immigration. The application of such legal means falls within the competence of the said body. Another agency under the Ministry of the Interior, the Office of Citizenship and Migration Affairs, is responsible for examining applications and making decisions regarding asylum seekers. Thus, in the event of a refusal to grant refugee status or alternative status, the person has the right to appeal this decision to the Administrative Court. Another internal affairs agency, the State Police, is responsible for cooperating with other agencies, such as the municipal police, in carrying out tasks to ensure public safety and order.

The second group includes the application of measures of the administrative process. And this is reflected in the activities of another institution subordinate to the Ministry of Internal Affairs, namely the Office for Citizenship and Migration Affairs, whose competence includes reviewing applications and making decisions for asylum seekers. Thus, in the event of a refusal to grant refugee status or alternative status, a person has the right to appeal this decision to the Administrative Court in accordance with the procedure established in the Administrative Proceedings.

The third group includes administrative-legal and procedural means applied in accordance with the Law on Administrative Liability, the Immigration law when establishing the fact of a person's presence in the country without valid documents (visa, residence permit) or a person wanted for committing a criminal offence in Latvia or another state and illegally staying in the country.

For example, the authors of this article reviewed statistics on applications for refugee and alternative status in an article published in 2016 [21].

The detained foreigner is placed either in the premises of the State Border Guard for temporary detention, or in an accommodation center, which may subsequently end with administrative procedures for determining refugee or alternative status. Several hundred such cases have been considered in the Administrative Court. In turn, when analyzing statistical indicators, in most cases - 95% of cases, alternative status or refugee status is refused, respectively, only 5% of the received applications for granting refugee or alternative status are satisfied [22].

The fourth group could include criminal legal remedies if a person residing illegally in the country commits a criminal offense.

The fifth group includes means of criminological prediction, which includes criminalization, decriminalization, penalization and depenalization and their measures. And finally, means of legal policy are regulated by the legislator.

Considering that one of the risks at the state border is illegal border crossing, it is necessary to consider statistical data on such illegal activity over a longer period of time. Illegal crossing of the state border entails criminal liability under Article 284 of the Criminal Law. Table 1 shows the changes in statistical data in the period from 2014 to 2024 [23]. *See Table 1.*

Year	*Criminal proceedings initiated in Latvia pursuant to Article 284 of the CL (unlawful crossing of the State border) in the period from 2014 to 2024*			
	Article 284 of CL	*Article 284, paragraph 1 of CL*	*Article 284, paragraph 1^1 of CL*	*Article 284, paragraph 2 of CL*
2014	32	12	-	20
2015	83	26	-	58
2016	101	27	-	74
2017	62	23	0	38
2018	46	15	3	28
2019	31	17	0	14
2020	8	*no date*	4	2
2021	46	9	0	35
2022	62	27	1	34
2023	142	63	0	79
2024	40	28	0	12

Table 1. Criminal proceedings initiated in Latvia pursuant to Article 284 of the CL (unlawful crossing of the State border) in the period from 2014 to 2024 [23].

From the contents of Table 1, it can be seen that over the past eleven years, an average of 57 criminal proceedings were opened and initiated annually for illegal crossing of the state border.

Most of these cases were initiated under the first part of Article 284 of the Criminal Law without qualifying elements. In turn, it should be mentioned that by

30.12.2023 the Article 284 of the Criminal Law was supplemented with the new prim paragraph, providing for liability for intentional illegal crossing of the state security, if the border violator has been banned from leaving the country in order to prevent a threat to national security (Article 284 of the Criminal Law), [17]. The highest number of crimes committed for illegal border crossing was registered in 2023 (142 cases). In turn, the lowest number of such crimes was registered in 2020 (8 cases) [23].

Note: Article 284, Paragraph 1.[1] of the Criminal Law has been included in the Criminal Law from 23 May 2017 [24].

When compiling statistics on identified cases of ensuring the possibility to illegally reside in the country (Article 285 of the Criminal Law) [23], it should be concluded that the largest number of such cases were identified in 2023 – 85 cases [23], while in 2020, such cases were not identified.

In turn, the number of cases of ensuring in bad faith to a person the possibility to acquire the legal right to reside in Latvia or another Member State of the EU has averaged 15.5 cases annually over the last eleven years (from 2014 to 2024). In 2021, the highest number of such cases was recorded–58 [23]. In contrast, no cases of ensuring in bad faith were detected in 2014 and 2020.

IV. CONCLUSION

1. The authors believe that the search for such new solutions should be the focus not only for the development of measures by the relevant competent authorities (primarily the responsible authorities of the State Border Guard of the Republic of Latvia or other EU Member States) in implementing their cooperation but also be in the centre of attention and monitoring of scientists and researchers. Cooperation could be improved both in the legal framework – in both the short-term and long-term perspective– and in the enhancement of technical and digital tools and means.

2. The range of measures to prevent illegal migration at the external border of Latvia is diverse and must be improved along with the development of new digital and technical means, as well as legal means in general.

3. Smart state border measures to help improve prevention of illegal migration are information technology tools, including the Visa Information System (VIS), the Entry/Exit System (EES), as well as European Travel Information and Authorization System (ETIAS). Digitization of personal data and new technical solutions for obtaining biometric data are important from the point of view of human rights, since the use of such tools must be balanced with human rights principles and current EU legal norms. Legal means of combating illegal migration, on the other hand, can be divided into four groups of measures. Those include depending on the sub-branch of law, administrative and criminal legal means and solutions can be distinguished.

4. However, there is a problem of uniformity of practice in the application of anti-illegal migration rights. Besides that, the legal tools and knowledge available to the State Border Guard and other law enforcement authorities in the application of this instrument (law enforcement) correspond to the level of development and requirements of the regulatory framework and modern social relations in general. The effectiveness of technical means can be significantly and negatively affected by deficiencies in personnel training or even by its absence.

5. Legal measures for effective control of illegal migration can be divided into several (5) groups: 1) authorities (within the limits of their competence established by law); 2) means of administrative process (examination of refugee or alternative status applications, administrative procedures); 3) Administrative-legal and procedural means (application of administrative liability); 4) criminal-legal and procedural means (application of criminal liability); 5) means of criminological prediction of iilegal migration (includes law policy measures – criminalization, dekriminalization, penalization, depanalization and wich the related measures); and finally 6) means of legal policy are regulated by the legislator.

V. ACKNOWLEDGMENTS

The authors of the article would like to thank the European Union Recovery and Resilience Facility, which funded the project. 5.2/1/i/0/2/24/1/CELA/003 “Implementation of consolidation and governance changes at Riga Technical University, Liepaja University, Rezekne Academy of Technology and Latvian Maritime Academy, and Liepaja Maritime College for progress towards excellence in higher education, science and innovation” /Project no. RTU-PA-2024/1-0042 “Development of methodological solutions for common safety risk management in the field of border management”/.

REFERENCES

[1] Ethic of security and surveillance technologies. EU publication, 2014, pp. 15-16. [Online]. Available: European Group on Ethics in Science and New Technologies (European Commission [Accessed Feb. 1, 2025].

[2] I. Nesterova. Security notion and impact on the development of data protection law. Protection values enshrined in Constitution: perspective of different field of law. Collection of research papers of the 77th International Scientific Conference of the University of Latvia. Riga: University of Latvia Press, 2019, pp. 357-364.

[3] A. Kjaksta, S. Struberga. Society security/in the book Latvian residents’ subjective perception of security: impact on security policy-making, 2021. Collective monograph. In Latvian. Scientific editors: prof. Dr.paed. Ž.Ozoliņa, prof. Dr.sc.pol. I.Reinholde-Riga: Latvian University Academic Press. [Online]. Available: *https://doi.org/10.22364/liesdu.05* [Accessed Feb. 22, 2025].

[4] Spanish police information statement on dismantling human trafficking network, February 2025. [Online]. Available: https://www.afp.com/en [Accessed February 22, 2025].

[5] Electronic identification as the 21st century standard for access to e-services, (without a year). In Latvian. [Online]. Available: https://blog.dokobit.com/lv/izglitojosi-raksti/elektroniska-identifikacija-ka-21-gadsimta-standarts-pieklusanai-e-pakalpojumiem/ [Accessed Feb. 20, 2025].

[6] R. Kozlovskis. Once the Smart Border is completed, we will have very serious support for Latvia's border security. Interview by the Minister of the Interior of the Republic of Latvia, 2024. [Online]. Available: https://www.la.lv/kozlovskis-kad-pabeigs-viedas-robezas-izbuvi-tad-mes-iegusim-loti-nopietnu-atbalstu-latvijas-robezas-apsardzei [Accessed Feb. 15, 2025].

[7] Smart Borders Pilot Project Report on the technical conclusions of the Pilot, 2015. [Online]. Available: https://home-affairs.ec.europa.eu/system/files/2020-09/smart_borders_pilot_report_on_the_technical_conclusions_en.pdf [Accessed Feb. 15, 2025].

[8] What is SIS and how does it work? European Commission, 2024. [Online]. Available: https://home-affairs.ec.europa.eu/policies/schengen/schengen-information-system/what-sis-and-how-does-it-work_en [Accessed Ferb. 15, 2025].

[9] Grenzüberschreitende polizeiliche Zusammenarbeit zwischen den Schengen-Staaten im EU Rahmen. Heranführung der Staaten Mittel-und Osteuropas, 1999. Seminar. In Deutsch. Weimar: Thüringerr Polizeiverwaltungsamt, s.147.

[10] Schengen Information System Operating Law. Schengen Information System Operating Law: the Law of the Republic of Latvia, no 102, 14 June, section 1., 2007. [Online]. Available: https://likumi.lv/ta/id/159481-sengenas-informacijas-sistemas-darbibas-likums [Accessed Feb.15, 2025].

[11] Judgment of the Court (Grand Chamber) of 31 January 2006. Commission of the European Communities v Kingdom of Spain, case C-503/03, 2007. [Online]. Available: https://curia.europa.eu/juris/liste.jsf?language=en&num=C-503/03 [Accessed Feb. 15, 2025].

[12] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry (2017) /Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC), no 767/2008, no 1077/2011. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2017/2226/oj/?locale=LV . [Accessed Feb.20, 2025].

[13] What is SIS and how does it work? (without a year). [Online]. Available: https://home-affairs.ec.europa.eu/policies/schengen/schengen-information-system/what-sis-and-how-does-it-work_en . [Accessed Feb. 20, 2025].

[14] Smart borders: EU Entry/Exit System (EES).European Commission, 2025. [Online]. Available: https://ec.europa.eu [Accessed Feb. 20, 2025].

[15] Schengen: New rules to make the area without internal border controls more resilient, 2021. [Online]. Available: https://latvia.representation.ec.europa.eu/jaunumi/sengena-jauni-noteikumi-ar-noluku-padarit-zonu-bez-ieksejas-robezkontroles-noturigaku-2021-12-14_lv . [Accessed Feb. 20, 2025].

[16] Costica Dumbrava. Artificial intelligence at EU border. European Parliamentary Research Service, 2021, pp. 690-706. [Online]. Available: DOI:10.2861/91831. [Accessed February 20, 2025].The Schengen area explained, 2025. [Online]. Available: https://www.consilium.europa.eu/lv/policies/schengen-are [Accessed Feb. 20, 2025].

[17] Video security, (without a year). Automatic Number Plate Recognition (ANPR). In Latvian. [Online]. Available: https://www.videodrosiba.lv/lv/anpr/ [Accessed Feb. 20, 2025].

[18] Criminal Law. Law of the Republic of Latvia. In Latvian, 1998. [Online]. Available: www.likumi.lv [Accessed Feb. 20, 2025].

[19] Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/399/oj/eng [Accessed Feb. 15, 2025].

[20] 9. International Scientific-Practical Conference "Border Security and Management", 2025. [Online]. Available: https://journals.rta.lv/index.php/BSM [Accessed Feb. 20, 2025].

[21] A. Gaveika, I. Bulgakova. Asylum law regulation and current events application in Latvia. International conference "Border Security and Management" issue, 2016, pp.53-63. [Online]. Availaible: https://doi.org/10.17770/bsm.v1i6.1700 [Accessed Feb. 24, 2025].

[22] Statistics of the Latvian Court Administration, 2025. [Online]. Available: Latvijas Tiesu Portāls [Accessed Feb. 20, 2025].

[23] Statistical data of the Information Centre of the Ministry of the Interior of the Republic of Latvia, 2014-2024. [Online]. Available: www.ic.iem.gov.lv/statistika [Accessed Feb. 22, 2025].

[24] Criminal Law. Law of the Republic of Latvia. In Latvian, 1998. [Online]. Available: www.likumi.lv [Accessed Feb. 20, 2025].

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 57-61

COVID-19, Infodemic and Cyber Security

Gabriela Belova
Faculty of Law and History
South-West University "Neofit Rilski"
Blagoevgrad, Bulgaria
gabrielabelova@gmail.com

Gergana Georgieva
Faculty of Law and History
South-West University "Neofit Rilski"
Blagoevgrad, Bulgaria
georgieva@law.swu.bg

Yosif Kochev
Faculty of Law and History
South-West University "Neofit Rilski"
Blagoevgrad, Bulgaria
kochev_88@law.swu.bg

Aleksandar Yankov
Faculty of Law and History
South-West University "Neofit Rilski"
Blagoevgrad, Bulgaria
alexander.yankov1990@gmail.com

Vladimir Babanov
Faculty of Law and History
South-West University "Neofit Rilski"
Blagoevgrad, Bulgaria
v.babanov@law.swu.bg

***Abstract* — The present article tries to trace the impact of some processes related to the COVID-19 pandemic on some areas of public life and in particular on national security. The analysis focuses on two main points, namely the infodemic and cybersecurity, as during COVID-19 they stood out as problems that will continue over time. The COVID-19 pandemic has been a challenge that requires the international community, governments and political elites to address multiple dimensions that go beyond just the effects on population health and also have an impact on security aspects. The starting point of the analysis is, of course, the social determinants of the right to health, which promote public health as an element of security and at the same time as one of the goals of sustainable development. In fact, it is precisely some of the determinants of the right to health that are subject to the infodemic, false or misleading information deliberately created to harm a person, social group, organization or country. Furthermore, the weaknesses the pandemic has so far highlighted point to an urgent need for a stronger international framework that would counteract the spread of misinformation and increasing complexity of cyberattacks. That calls for an all-rounded strategy that includes increased international cooperation, public awareness, and the application of cutting-edge technical solutions. An appropriate methodology has been used in view of the delicate matter of health, which becomes even more vulnerable when subjected to infodemic or cybercrime. The main conclusion of the authors is that, in addition to improving international legislation with a view to preparing for and preventing future pandemics, more attention should also be paid to the phenomena that accompany them, such as the infodemic and cybercrime. This is of utmost importance, as they could be expected to develop on a much larger scale in possible future pandemics. The international community and national elites should discuss and take measures to deal with these phenomena.**

Keywords* — *COVID-19, cybersecurity, infodemic, post-pandemic world.

I. Introduction

Today, humanity has breathed a sigh of relief that the COVID-19 pandemic is already over. Public health has regained its position and the international community has refocused its efforts on achieving Goal 3 of the Sustainable Development Goals, ensuring a healthy lifestyle and promoting well-being for all during the whole life. However, this does not mean that some aspects related to it, such as infodemic and cybersecurity, should not be carefully analyzed, moreover, they will continue to have an impact on the life of modern society. It is important to follow and outline some trends, as well as the necessity that definite measures should be taken by the international community, by the countries and national elites in order to overcome the negative consequences. This is of utmost importance, as they could be expected to become of greater importance in possible future pandemics.

II. Materials and Methods

The present article aims critically to analyze the COVID-19 pandemic health issues in terms of fake news and disinformation as well as cybersecurity.

The issue has been explored in recent years but still needs further attention and research. Due to the sensitive nature of the issue, a complex methodology has been

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8479
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

used, combining several approaches and including analytical, teleological, historical and comparative methods.

To achieve the goals of the research, the article also uses some statistical data collected from the official websites of European and national institutions, the observation and analysis of which allows the authors to reach scientifically based conclusions regarding the level of infodemic and cybersecurity.

III. RESULTS AND DISCUSSION

A. COVID-19 and social determinants of the right to health

The UN's Sustainable Development Goals were adopted on September 25, 2015, by the 193 countries in the UN General Assembly as a continuation of the Millennium Goals. Just as they call for a focus on the linkages between development policy sectors, the pandemic has revealed complex global interdependencies that reinforce the lines of ethnic, economic, and gender inequality in society.

Goal No. 3, a part of the agenda 'Transforming our world', has been defined as ensuring a healthy lifestyle and promoting well-being for all during their whole life. Its achievement is directly related to the improvement of the so-called social determinants of the right to health and health care which are mostly understood as structural factors and everyday living conditions that significantly determine existing health inequities within and between countries.

One of the most important determinants of the right to health is undoubtedly nutrition and a healthy lifestyle. The right to health includes not only the provision of a sufficient quantity of safe food, but it also raises the question about the 'double standard' regarding the quality and ingredients of food in some EU Member states, particularly V-4 countries and Bulgaria and Romania as well [1]. In recent years, global prices of basic food products have increased sharply, causing serious concern among the governments of some countries, as well as among non-governmental organizations. According to forecasts of the United Nations Population Fund (UNFRA), by the middle of the 21st century, the population of the planet is expected to reach 9 billion people and lead to a shortage of agricultural land, water, energy resources, food, which in turn would expectedly increase the prices of the main food products from the consumer basket [2]. However, these data and facts regarding the livelihood of the population as one of the most important social determinants of the right to health, have become the basis of a number of fake news related to the pandemic of COVID-19.

B. Infodemic

As Reddy and Gupta rightly point out, in the era of the COVID-19 pandemic there is an abundance of information, leading to the so-called infodemic, and such a situation requires an adequate response and providing people with accurate and verified information [3]. This is the first pandemic to take place in a time of social media boom, which basically means everyone knows about the coronavirus, everyone is talking about it, and everyone feels able to give some advice about it. The fear associated with the pandemic is unprecedented, so the infodemic may cause more harm than good for public awareness [4], [5]. Some authors even use the term 'netizens' in articles devoted to the pandemic to emphasize the importance of social networks in relation to individuals, equating it to citizenship [6].

It is hardly a coincidence that conspiracy theories of the Malthusian type and a significant portion of the pieces of fake news have emerged on the occasion of the COVID-19 pandemic. The world in the 21st century has noticed a revival of extreme views that wars, epidemics, and diseases keep population growth under control and should be evaluated positively. In the new context of COVID-19, some even portray the Bill and Melinda Gates Foundation as part of a global conspiracy. Bulgaria has not been isolated from the spread of fake news either, and unfortunately, the population has been susceptible to such information. According to a survey conducted in November 2020 approximately 40% of Bulgarians agreed that the coronavirus was a biological weapon created to reduce the population of the Earth and this is relatively a high percentage [7]. Certain internet sites distribute controversial statements by the member of the Chamber of Deputies of Italy, Sara Cunial, who proposes that the International Criminal Court indicted Bill Gates. The Italian newspaper La Repubblica quoted Cunial's May 14, 2020 speech. In her comment on the prime minister, Giuseppe Conte she appeals: "The next time philanthropist Bill Gates calls you, refer him straight to the International Criminal Court for crimes against humanity" [8].

It should be also emphasized that since the outbreak of the COVID-19 pandemic, social media has played an essential role in the genesis of anti-China sentiments around the world. A restaurant chain Kwong Wing Catering in a Facebook message dated January 28, 2020, informed that it will not serve Mandarin-speaking customers as part of anti-epidemic measures [9]. A few days earlier, misinformation that Chinese travelers from Wuhan with fever had slipped through the quarantine at Kansai International Airport was spread on various social media channels in Japan [10]. Conspiracy theories, derogatory attitudes towards eating habits, prejudice against Chinese socio-cultural norms, and calls for the isolation of the entire nation posted on social media are in many cases openly discriminatory and racist in nature. Prolonged stigmatization, stress and multiple mental problems are among the severe consequences of the irresponsible behavior of some media and netizens [6]. In this sense, health service providers, together with mass media, should take responsibility for providing the right information and for creating effective communication with citizens in order to limit the 'infodemic'.

The 'infodemic' proves to be a constantly evolving phenomenon that has led to the appearance of various categories of disinformation. Each of them has a unique

approach and purpose. In this regard [11] points out a systemic classification of fake information which distinguishes three main types. The first one is the so called 'misinformation' which is fake information that is spread without malicious intent. The classic 'disinformation' is fake information which spreads with the purpose of damage infliction. The third type of disinformation, called 'malinformation', is actually a true information which is not meant for public access, but has been openly spread by malicious actors who seek to do harm.

The automation of disinformation generation through the usage of AI in the last few years resulted in a flood of incorrect online content without verifiable sources. Common approach of the malicious actors is mixing and presenting the disinformation in such a way that makes it appear factual. The utilization of satire and parody makes fake information appear harmless but could possibly lead to establishing of fake correlation between unrelated circumstances or people. Misleading content, imposing of imaginary context, fabricated statements and manipulated content are merely a few subcategories in the three classes of disinformation.

In the first days of the COVID-19 outbreak in China, a 'media panic' has been characterized by a flood of fake news and misinformation that has metastasized faster than the coronavirus itself. Not by chance, WHO Director-General Tedros Ghebreyesus on February 15, 2020, during the Munich Security Conference stated that the organization is fighting not only the epidemic, but also the infodemic, which instils fear and panic through uncontrolled rumors and sensational news [12]. The discrepancy with real facts and data was mainly due to online content gleaned from unreliable and dubious but easily accessible social media. Immediately after the outbreak of COVID-19, many bloggers, groups or users on YouTube, WhatsApp, Facebook, Instagram and Twitter began to profit from the popularity of the coronavirus by provoking impulsive and unpredictable actions [13]. Unfortunately, the development of social media is destroying some boundaries that prevent the spread of fake news in democratic countries [14], [15]. As sensational and gruesome content gets the most attention on social media, several users are using COVID-19 to gain cheap popularity or purposefully sow confusion and panic. They provoke mental states such as anxiety, phobia, panic, depression, mania, irritability, delusion about the existence of COVID-19 symptoms and other paranoid ideas. Consumers of health services are too confused and worried not only because of the information about COVID-19 itself, but also because of the behavior of the media actors.

C. Cybercrime

Another challenge to the right to health in the context of the COVID-19 pandemic was cybercrime. As the fears of the coronavirus infection rapidly occupy the minds of the global population, cybercriminals are looking to use every opportunity to extract all kinds of benefits from their victims on the occasion of services and products related to COVID-19. Cybercriminals, for example, could seek information about treatments, tests or vaccines related to the coronavirus to sell on the black market, encrypt sensitive data and hold it for ransom, or simply disrupt the interoperability of the institution [16]. Interpol Secretary Jürgen Stock stated that hospitals and medical organizations around the world are constantly working to preserve the well-being of individuals affected by the coronavirus who have become targets for ruthless cybercriminals trying to make a profit at the expense of sick patients [17].

The biggest and most disturbing incident to date happened on March 13, 2020, at the University Hospital in Brno (Czech Republic), which suffered an extremely serious cyber attack in the midst of the coronavirus infection epidemic, which led to the suspension of planned operations [18]. As a result of the cyber attack, the hospital was unable to transfer information from key clinical systems to its database and was forced to shut down its IT systems and transfer emergency patients to another medical facility in the city. It should be borne in mind that the hospital was the second largest national site of strategic importance in the field of healthcare and at the time of the attack it was among the most important testing centers for COVID-19 in the Czech Republic. "The public address system at the hospital began repeating the message that all staff should immediately shut down all computers due to a cyber attack", reported a cyber security expert who was waiting at the hospital for surgery at the same time [19]. The cyber attack did not affect work related to coronavirus testing, but it did cause disruption to the hospital's extremely stressful and busy schedule.

Although the exact origin of the attack was unknown, signs point to the possibility that the hospital's IT infrastructure was encrypted by ransomware. The accident was confirmed by the Czech National Cyber and Information Security Agency (NÚKIB), which had been cooperating throughout with law enforcement and hospital staff to succeed in returning the facility to full operational readiness [16].

After the incident in the Czech Republic, experts warn that the spread of the coronavirus infection provides fertile ground for cybercrimes of all kinds. The cyber attack against the hospital in Brno is causing serious concern among specialists, primarily due to the fact that so far online crime related to COVID-19 has been primarily limited to phishing attacks (targeted emails using catchy headlines and attachments to inject malicious software) and disinformation campaigns. After the case of the hospital in Brno, experts warn that the spread of the coronavirus infection provides fertile ground for cybercrimes of all kinds. According to experts, to date, there has never been a cyber attack on a healthcare or medical facility that has directly resulted in loss of life, but it is only a matter of time before it happens [16].

The consequences of the pandemic can only be compared to those caused by the two world wars in the twentieth century. It is assumed that for a better assessment of the situation, it should be analyzed from different points of view. First of all, the health consequences should undoubtedly be taken into account, while in second place are the economic losses. In addition, the sheer scale of the crisis and the impact it is having is naturally causing a lot of fear, uncertainty and anxiety around the world. As some researchers point out, crises usually evoke apathy, conformity, or overenthusiasm associated with some savior [20], [21]. In the case of COVID-19, there are serious psycho-social consequences caused not only by the disease itself, but also by social isolation, disrupted work and family habits, and economic instability. In a survey made in 2020 by the Kaiser Family Foundation, 45% of adults in the United States believe that anxiety and stress related to the coronavirus have had a negative impact on their mental health [22].

D. Post-pandemic situation

Hopes that perhaps with the end of the COVID-19 pandemic and the return to normal life and the normal functioning of state bodies and institutions, cybercrimes in health systems will decrease, unfortunately, did not come true. With technological advances and the deteriorating geopolitical situation, nowadays we are witnessing even an increase in cybercrime. This is a fact even in well-developed democratic countries. As the National Advisor for Cyber security and Risk of American Hospital Association John Riggi stated in 2024 386 health care cyber-attacks were reported [23]. Compared to the previous several years this was the worst year ever for breaches in health care [24]. A careful analysis shows that nowadays ransomware attacks are not just data theft or financial crimes, they become real threat-to-life crimes. A significant part of them threaten the safety of patients in the hospital as they are designed to stop the life support systems, causing maximum delay of medical services or disruption to patient care. Hospitals strongly depend on a third party to deliver critical, life-saving functions and clinical care. In 2023 in the United States due to an attack on third party for health care, a 287% increase in cyber attacks has been reported compared to 2022 [25]. And it should be noted that third-party data breaches pounded health care more than any other sector [26]. And this becomes not an isolated situation in one country but a global concern as the World Health Organization has alarmed that the increased ransomware attacks are putting the world's healthcare infrastructure at critical risk, endangering patient safety and destabilizing healthcare systems [27], [28].

The WHO Director-General Tedros emphasised the severe impact of cyberattacks on hospitals and healthcare services, calling for urgent and collective global action to address this growing crisis. "Ransomware and other cyberattacks on hospitals and other health facilities are not just issues of security and confidentiality, they can be issues of life and death," he said. And added that just as viruses do not respect borders, nor do cyberattacks and therefore international cooperation is essential [28].

IV. CONCLUSIONS

The COVID-19 pandemic has prompted the international community to take measures and prepare a draft convention on pandemic prevention, preparedness and response in case of possible future pandemics [29], [30]. This is undoubtedly a step forward in the development of international legislation. However, it seems that it is necessary to take timely measures to effectively counter the infodemic and cybersecurity threats, which are likely to increase in future pandemics. While improving international legislation with a view to preparing for and preventing future pandemics, more attention should also be paid to the phenomena that accompany it, such as misinformation and cybercrime. It is the responsibility of all actors – the international community, states and national elites to discuss and to take appropriate measures to deal with these contemporary phenomena.

REFERENCES

[1] BTA "Bulgarian MEPs Urge European Commission to Take Measures against Double Standards for Foods," Sep. 4, 2017. [Online]. Available: BTA :: Bulgarian MEPs Urge European Commission to Take Measures against Double Standards for Foods. [Accessed Dec. 30, 2024].

[2] UN Department of Economic and Social Affairs, "World Population projected to reach 9.8 Billion by 2050, and 11,2 billion in 2100". UN Population Division/DESA/UNFRA. [Online]. Available: World population projected to reach 9.8 billion in 2050, and 11.2 billion in 2100 | United Nations. [Accessed Dec. 10, 2024].

[3] B.V. Reddy and A. Gupta, "Importance of effective communication during COVID-19 infodemic." *Journal of Family medicine and primary care*, vol. 9, no.8 pp. 3793-3796, 25 Aug. 2020. [Online]. Available: Importance of effective communication during COVID-19 infodemic - PMC [Accessed Nov. 15, 2024], https://doi.org/10.4103/jfmpc.jfmpc_719_20.

[4] R. Nikolova and A. Yankov, "COVID-19, Psychosocial Effects and Fake News", International conference Knowledge – Based Organization, Vol.27, Issue 2, pp. 176-179, June 2021. [Online]. Available: ResearchGate, (PDF) COVID-19, Psychosocial Effects and Fake News [Accessed Dec. 16, 2024], https://doi.org/10.2478/kbo-2021-0069.

[5] A. Yankov, "Distinction between the concepts of "freedom of expression" and "hate speech" (In Bulgarian), *International Politics*, vol. 2/2021, pp. 57-64. [Online]. Available: Publications (swu.bg). [Accessed Nov. 15, 2024].

[6] S. Dubey, P. Biswas, R. Ghosh, S. Chatterjee, M. J. Dubey, S. Chatterjee, D. Lahiri and C.J. Lavie, "Psychosocial impact of COVID-19", *Diabetes & metabolic syndrome,* vol. 14, no 5, pp. 779-788, May 2020. Available: PubMed, Psychosocial impact of COVID-19 - PubMed. [Accessed Nov. 26, 2024], doi: 10.1016/j.dsx.2020.05.035. PMCID: PMC7255207.

[7] BNR "Trend: 40% of Bulgarians believe COVID-19 is a Biological Weapon", Nov. 24, 2020. [Online]. Available: Trend: 40% of Bulgarians believe Covid-19 is biological weapon - News. [Accessed Sept. 17, 2023].

[8] V. Antonova "Bill Gates, the Villain", [Online].Available: Bill Gates, the Villain | AEJ-Bulgaria. Jan. 20, 2021. [Accessed Sept. 24, 2023].

[9] R.Y. Chung and M.M. Li, "Anti-Chinese sentiment during the 2019-nCoV outbreak", *Lancet*, vol. 395, Issue 10225 pp. 686–687, Feb. 12, 2020. [Online]. Available: PubMed, Anti-Chinese

sentiment during the 2019-nCoV outbreak - PMC. [Accessed Sep. 17, 2023]. https:// doi: 10.1016/S0140-6736(20)30358-5.

[10] K. Shimizu, "2019-nCoV, fake news, and racism", *Lancet*, vol. 395, Issue 10225, pp. 685–686. Feb.29, 2020. [Online]. Available: PubMed, 2019-nCoV, fake news, and racism - The Lancet. [Accessed Sep.18, 2023]. https://doi: 10.1016/S0140-6736(20)30357-3.

[11] J. Harsin, "Disinformation as a Context-Bound Phenomenon: Toward a Contextual Framework", Communication Theory vol. 33, no. 1, pp. 1–23, 2023. [Online]. Available: https://academic.oup.com/ct/article/33/1/1/6759692 . [Accessed Jan. 21, 2025].

[12] J. Zarocostas, "How to fight an infodemic", *Lancet*, vol. 395, Issue 10225, p. 676, Feb.29, 2020. [Online]. Available: How to fight an infodemic - The Lancet. [Accessed Sep.18, 2023]. https://doi:10.1016/S0140-6736(20)30461-X.

[13] R.M. Merchant and N. Lurie, "Social media and emergency preparedness in response to novel coronavirus", JAMA. May 26, 2020. [Online]. Available: PubMed Social Media and Emergency Preparedness in Response to Novel Coronavirus PubMed [Accessed Sep. 26, 2023]. https://doi:10.1001/jama.2020.4469.

[14] G. Belova and G. Georgieva, "Fake News as a Threat to National Security", International conference Knowledge – Based Organization, vol. 24, Issue 1, pp. 19-22, June 2018. [Online]. Available: ResearchGate (PDF) Fake News as a Threat to National Security [Accessed Aug. 4, 2022]. https://DOI:10.1515/kbo-2018-0002.

[15] N. Popov, "Globalization and Security of the Individual in the National State", (In Bulgarian), *Law, Politics, Administration*, vol. 8, issue 2, pp. 10-14, 2021. [Online]. Available: CEEOL - Article Detail. [Accessed Aug. 20, 2022].

[16] G. Belova, N. Marin and Y. Kochev, "COVID-19 and cybercrimes against healthcare" (In Bulgarian), *National Security*, Issue 5, pp. 34-40, 2020. ISSN 2682-9983. [Online]. Available: https://nacionalna-sigurnost.bg/sdm_downloads/cyber-crimes/. [Accessed Sep.18, 2022].

[17] INTERPOL "Cybercriminals targeting critical healthcare institutions with ransomware", Apr. 4, 2020. [Online]. Available: https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware. [Accessed Sep.18, 2022].

[18] Security "Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak", Mar. 17, 2020. [Online]. Available: Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak | 2020-03-17 | Security Magazine. [Accessed Oct. 4, 2022].

[19] M. Burges, "Hackers are targeting hospitals crippled by coronavirus", Security, Mar. 22, 2020. [Online]. Available: Hackers are targeting hospitals crippled by coronavirus | WIRED. [Accessed Oct.6, 2022].

[20] A. Hristova and G. Georgieva, "New Research and Technology Development", Kutafin Law Review, vol.4, Issue 2, pp. 388-397, 2017. [Online]. Available: New Research and Technology Development: Some Legal and Ethical Issues | Hristova | Kutafin Law Review. [Accessed Sep. 18, 2022]. https://doi.org/10.17803/2313-5395.2017.2.8.388-397.

[21] T. Koburov, Situational foreign political analysis in the field of security. (In Bulgarian). Sofia, King, 2009, p.109.

[22] "KFF Health Tracking Poll – Early April 2020: The Impact of Coronavirus on life in America", Apr. 2, 2020. [Online]. Available: KFF Health Tracking Poll - Early April 2020: The Impact Of Coronavirus On Life In America | KFF. [Accessed Oct. 18, 2022].

[23] J. Riggi, "A Look at 2024's Health Care Cybersecurity Challenges", Oct. 7, 2024. [Online]. Available: A Look at 2024's Health Care Cybersecurity Challenges | AHA News. [Accessed Nov. 26, 2024].

[24] J. Riggi, "Ransomware attacks on Hospitals Have Changed", [Online]. Available: Ransomware Attacks on Hospitals Have Changed | Cybersecurity | Center | AHA. [Accessed Nov. 25, 2024].

[25] T. Broderick, "Healthcare data breaches hit new highs in 2023", Modern Healthcare, Jan. 25, 2024. [Online]. Available: Healthcare data breaches hit new highs in 2023 | Modern Healthcare. [Accessed Nov. 25, 2024].

[26] S. Alder, "Healthcare Experiences More Third-Party Data Breaches Than Any Other Sector," *HIPAA Journal*, Mar. 4, 2024. [Online]. Available: Healthcare Experiences More Third-Party Data Breaches Than Any Other Sector. [Accessed Nov. 26, 2024].

[27] A. Koceva and D. Kostadinova, "A comparative analysis on apology speech acts in American English and Macedonian", PALMK, vol. 6, no. 12, pp. 37-45, Dec. 2021. [Online]. Available: https://js.ugd.edu.mk/index.php/PAL/article/view/4757. [Accessed Jan. 27, 2025]. https://doi.org/10.46763/palim.

[28] V. Mishra, "Cyberattacks on Healthcare: A Global Threat That Can't Be Ignored", UN News Global Perspectives Human Stories, Nov. 8, 2024. [Online]. Available: Cyberattacks on healthcare: A global threat that can't be ignored | UN News. [Accessed Dec. 23, 2024].

[29] Kiryakova-Dineva, Teodora, and Ruska Bozhkova. "Public Health Risk Environment for Bulgarian Smes (Guest Houses and Family Hotels) in the COVID-19 Pandemic." Advances in Hospitality, Tourism, and the Services Industry, pp. 77–102, 2021. [Online]. Available: https://www.igi-global.com/chapter/public-health-risk-environment-for-bulgarian-smes-guest-houses-and-family-hotels-in-the-covid-19-pandemic/280891. [Accessed Jan. 30, 2025]. https://doi.org/10.4018/978-1-7998-6996-2.ch004.

[30] Stoykova, P., "Education as a cause for participation in politics: A case study in Bulgaria". Balkan Social Science Review, 18, pp.299–323, 2021. [Online]. Available: https://js.ugd.edu.mk/index.php/BSSR/article/view/4819. [Accessed Jan. 31, 2025]. https://doi.org/10.46763/BSSR2118299s.

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference . 2025. Volume V, 63-68

Design of the Training – Approach for Identification of the Requirements to the Educational Process in the Military Education System

Daniel Berchev
Research and Innovation Institute
Vasil Levski National Military University
Veliko Tarnovo, Bulgaria
dberchev@nvu.bg

Milko Stefanov
Information and Security Affiliate
Rakovski National Defense College
Sofia, Bulgaria
m.j.stefanov@rndc.bg

***Abstract* — This article considers the design phase of the systems approach to training as a logical link between the results of the learning analysis and the development phase. In this sense, the object of research is the systems approach to training, and its subject is the design of training, in the context of the military education system. The purpose of the article is to provide: (1) an understanding of the content and approach for implementing the training design phase as an element of the systems approach to training; (2) analyzing different approaches for implementing the training design phase; and (3) observations on the features of the training design phase. In the conclusion of the article, the authors substantiate their view that training design, as a stage of the implementation of the systems approach, requires the identification of resources, goals, sequence and environment of training to meet the requirements of the military education system.**

Keywords* — *education, military education system, systems approach to training, training design.

I. Introduction

Military education system, as part of the education system of the Republic of Bulgaria, is called to ensure the preparation of personnel in regulated professions in the field of security, such as: "Officer for tactical level of management", "Officer for operational level of management" and "Defense and Armed Forces Strategic Command Officer". The structuring of the military education system ensures lifelong learning in the context of training officers for the needs of the Bulgarian Army and the Armed Forces (AF) of the country. The functioning of the military education system is closely related to a set of responsible institutions, determined to manage the capabilities and resources, to build the way and contribute to the achievement of the educational goal of the society and the specific goals of the Bulgarian Army and the AF as a whole.

At the entrance to the military education system are the higher military schools, in particular the Vasil Levski National Military University (NMU "V. Levski"), which predetermines their responsibility in designing the training of future officers. For decades, military education and training in military academies was clearly influenced by the Cold War paradigm. With our country's full membership in NATO and the European Union (EU), the requirements for military education and training have changed, and a frequently asked question has been: What can be learned from other armies about how to better prepare our future officers for the full range of operations?

Approaches to training and organizing the armed forces of other countries that are part of NATO and/or the EU reflect the requirements placed on them by the respective security environment. Every country faces strategic circumstances that require its armed forces to prepare for a combination of internal and external threats. In this context, the role of the institutions (Ministry of Defense, military academies, higher military schools, military colleges, training centers, etc.) is to provide an appropriate problem-solving framework to be used by military personnel (in particular, officer-cadets, trained in higher military schools) and units when asymmetric and conventional threats present challenges that existing methods do not adequately address. This highlights the need to apply new approaches to address the changing requirements for the capabilities of the AF, and for this it is important to ensure an understanding of the processes related to education and training taking place within the military education system,

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8465
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

which will provide adequate solutions for their improvement.

Taking into account all the peculiarities in the formation of the professional competences of the future officers at the NMU "V. Levski", we decided to approach this problem from the position of the systemic approach. Therefore, in this publication, the object of research is the systems approach to training, and its subject is the design of training, in the context of the military education system. In this sense, the purpose of the article is to provide: (1) an understanding of the content and approach for implementing the training design phase as an element of the systems approach to training; (2) analyzing different approaches for implementing the training design phase; and (3) observations on the features of the training design phase.

II. Materials and Methods

A systems analysis was applied when considering the training system as consisting of various elements (goals, content, methods, means, assessment), which are interconnected and influence each other.

A comparative analysis was made of different approaches to training design, presented by different authors and organizations (Hamza, Dhawan, US Army, British JSP 822), as well as of the definitions of "education" and "training" given by different authors and organizations (Armstrong & Taylor, NATO, US Army, British Army, Bulgarian doctrine).

Regulatory and departmental documents, curricula and programs, NATO documents, as well as scientific publications were analyzed.

A descriptive analysis was made of the phases of training design and the features of training in the military education system, which must be taken into account when designing training.

III. Results and Discussion

1. Education and training in the context of the military education system

There is debate about the relative value of "education" versus "training." Many critics argue that the various military schools should be training officers for their next assignment, rather than training them for greater professional contribution at some unspecified future time and place. Others insist that military education should focus on operational military matters to the exclusion of "soft" subjects such as international relations, economics, governance, etc. [1, p. 21].

The identification of "education" and "training" in the context of the military education system is common, but in their etymological and didactic sense the two concepts differ. This requires that the characteristic features of each of the concepts be deduced. As a starting point for our reasoning, we will indicate a few definitions for the two terms.

When it comes to civilian organizations, the primary purpose of learning and development as an organizational process is to support collective progress by collaboratively, expertly and ethically stimulating and facilitating learning and the acquisition of knowledge that supports business objectives, develops individual potential and respects and builds the diversity. In this regard, Armstrong and Taylor define education and training as components of learning and development. The latter are defined as the process of ensuring that an organization has the knowledgeable, skilled and engaged workforce it needs. The definitions of education and training that the two authors state are as follows:

- Training – the systematic application of formal processes to transfer knowledge and help people acquire the skills they need to perform their jobs satisfactorily.

- Education – the development of knowledge, values and understanding needed in all aspects of life, rather than knowledge and skills related to particular fields of activity [2, p. 284].

Although true, the above definitions can be seen as restrictive in the context of the Bulgarian Army and the Armed Forces of our country. Army training is the act of acquiring, maintaining, or improving knowledge, skills, and attitudes to achieve specified standards. Army training is a combination of training, education and experience. In virtually all military schools, professional development programs include elements of both education and training. Coordination between them implies achieving success across the learning continuum, by forming a synergistic effect, as personnel gain experience and develop individually over time, acquiring and performing progressively higher skills and responsibilities as they advance in their careers [3, pp. 21-22].

In the NATO documents governing the spectrum of education, training, exercise and evaluation (ETEE) activities, education and training are defined as follows:

- Education: Systematic training of individuals that will improve and develop their knowledge, skills and competencies to perform duties and tasks associated with a position/role. It is a developmental activity that enables individuals to take a reasonable response in any situation, including unpredictable ones.

- Training: Individual training is the development, improvement and retention of the skills and knowledge necessary to perform specific duties and tasks. Individual training is a learned response to a predictable situation (skills). Collective training is designed to prepare teams, units, and other elements to perform military tasks in accordance with specified standards. Collective training includes procedural training and practical application of doctrine, plans and procedures to acquire and maintain collective tactical, operational and strategic capabilities [4, p. 2].

As such, the NATO training spectrum is defined as having an individual focus linked to collective knowledge.

The individual focus is described by two elements: education and individual training. The collective side includes collective training and exercises [5, p. 6].

The US Army Strategic Training Framework considers Army training and education as elements of professional development programs and defines them as follows:

- Training is a learning event designed to develop, maintain, or improve the ability of individuals or units to perform specific tasks or skills. Viewed through the lens of "psychomotor, cognitive, and affective (related to moods, feelings, and attitudes) learning," training is largely defined by psychomotor learning and promotes mastery of established performance standards in the operational environment.
- Education imparts both specific and general knowledge and develops habits of mind applicable to a wide range of activities. Viewed through the lens of 'psychomotor, cognitive, affective learning', education is largely defined by cognitive learning and promotes broadening of horizons, use of different perspectives, critical and reflective analysis, abstract reasoning and innovative thinking, especially in relation to complex, ill-structured or non-linear problems.

For the purposes of the British Army, the Training and Education Manual (JSP 822) states that 'training' covers any training, education, learning or development activity, whether individual or collective, which is designed to meet the needs of cadres users [6, p. 4].

The Doctrine for the Training of the Armed Forces of the Republic of Bulgaria (NP-7) considers "training" as "a process of transmission and assimilation of knowledge, skills and habits for the acquisition of education, qualification, competences, appropriate motivation, optimal physical and mental qualities, corresponding of the needs of the armed forces to build the necessary operational capabilities" [7, p. 51].

NMU "V. Levski", as a higher state school, conducts training for cadets to acquire higher education at the educational-qualification degree "Bachelor" in the field of higher education "Security and Defense", professional direction "Military Affairs" in the specialties of the regulated profession "officer for tactical level of management". The state requirements related to this are defined by an ordinance adopted by Decree of the Council of Ministers (DCM) No. 205 of 30.08.2012. It states that higher education in specialties from the regulated profession "officer for tactical level of management" is acquired through training of officer-cadets in full-time/part-time form of education. In addition, the training and outcomes are said to be compliant with level 6, sub-level 6 'b' of the National Qualifications Framework (NQF). It is an integrated qualifications framework and is fully aligned with the Qualifications Framework in the European Higher Education Area and the European Qualifications Framework for Lifelong Learning. In the NQF, among others, the general descriptors for the educational and qualification degree "Bachelor" are listed, based on the results of the study and the acquired knowledge, skills and competences:

- knowledge – is defined as theoretical and/or factual;

- skills – described as cognitive (involving use of logical, intuitive and creative thinking) and practical (involving dexterity and use of methods, materials, equipment and tools);

- the competences – personal and professional, are described in view of the degree of taking responsibility and independence [8].

The training in specialties of the regulated profession "officer for tactical management level" is carried out according to curricula that are approved by the Minister of Defense in coordination with the Minister of Education and Science. The curriculum includes compulsory, elective and optional subjects. Compulsory study disciplines provide broad-based and specialized training, building professional competences. They are separated thematically into groups with a minimum timetable, as follows: Basic military training (150 academic hours); General military training (200 academic hours); Special military training (700 academic hours); National Security, Resource Management and Fundamentals of Law (150 academic hours); Educational practice and internship (120 academic hours); Language, leadership and physical training (700 academic hours). On the other hand, elective courses provide specific knowledge and competences, and optional courses provide the opportunity to acquire knowledge and skills in various scientific fields [9].

Structured in this way, training should provide:

1. obtaining broad-based and specialized professional training in the professional field "Military Affairs";

2. acquisition of adaptability skills in accordance with the changing conditions of professional realization;

3. acquisition of skills for independent professional work and team work;

4. conditions for educational mobility and international comparability of acquired knowledge and acquired capabilities [9].

From the analysis of the above-mentioned features of education and training in the context of the military education system, we can summarize that:

- these are processes that are well defined, which means that the two concepts (education and training) should not be used interchangeably;

- the training and education of people in defense is an activity of particular importance for building defense capabilities;

- through the training of officer-cadets in the higher military schools, emphasis is placed on the people in the

defense, who are the basis of the operational capabilities of the Armed Forces of our country.

2. What is a systems approach to training and why should it be implemented?

The systems approach to training (SAT) is widely used in the organization and direction of all learning product development activities by both civilian and military educational institutions. Such learning products can be individual courses (short-term and long-term), training modules, training programs in a specific discipline from a curriculum, as well as for the entire training course for obtaining an educational-qualification degree in higher schools.

The SAT is used in the analysis, design, delivery, provision, direction and management of defense training and education [6, p. 8].

To create an effective and efficient training program, NATO policy applicable to member states is to use a SAT to design and develop a training product that is focused on the core tasks, relevant job requirements and objectives of the training necessary to perform a certain activity [10, p. 5]. In this regard, at the core of the training and education process woven into the military education system is the application of a SAT that will ensure that our training and education is relevant, efficient and effective.

All training systems are unique. Accordingly, the SAT process is not designed to be prescriptive or restrictive [11, p. 2]. In the literature, the general view is that the systems approach is a process that encompasses five interdependent phases – analysis, design, development, implementation and evaluation. Each one of them is based on the results of the previous one. However, they are not sequential, and a change in each requires review and may require adjustments to previous phases.

Although evaluation is usually listed as the last step, it is carried out throughout the whole process of the SAT [12, p. 5]. This means that those who develop the training products can move in and out of each phase. The continuous formation of evaluation of the products of the process of the SAT, together with their approval, serve to eliminate or reduce deviations from the goal of training [3, p. 45].

3. Training design as an element of the system approach to training

The "Design" phase is a decision-making phase [12, p. 3]. It can be defined as the logical connecting element between the results obtained from "Analysis" and "Development", which are the main elements of the SAT.

There are different understandings of what "Design" should encompass. One of these views is that of Hamza [13], who states that design is an outline of all the details related to the training process: "what, where, who, when and how", for use by coordinators, curriculum developers and teachers (instructors). According to him, there are five main components of training design:

- Learning outcomes;
- Training Materials;
- Trainers and Content Experts (Subject Matter Experts);
- Training Methods;
- Logistics [13, p. 23].

Dhawan [12] points out that in the design phase, we perform three important activities:

1. We define what the student needs to learn in class and how to translate that learning into practical activity. In this way, we form the learning objectives.

2. We determine what the teaching material and teaching methods should be.

3. We develop a plan (method) for assessing the student's competence to perform the specified activity [12, p. 3].

For the needs of the US Army, TRADOC Regulation 350-70 (2017) states that the design phase identifies all resource requirements, learning environment, learning objectives, test items, learning sequence, and assessment and/or graduation requirements of the trainees. The detailed plan developed must be consistent with the users of the cadres. It defines when, where, and how training outcomes are achieved to meet Army requirements. It also determines the resources needed to develop, distribute, implement, and evaluate learning products [3, p. 49].

In its most detailed form, the design phase is presented in Volume 2: Defense Individual Training V3.0, part of the Training and Education Manual JSP 822 (V7.0 Feb 24). In it, the design of training is defined as the second phase of the application of the SAT. The manual provides guidance on the activities and the results resulting from them. Training design is described as a three-step process that formulates the training objectives based on the results of the Analysis.

During the first stage, the main goals are formed, based on the already established standards and the conditions for their implementation. In addition, the supporting objectives and main details of the training are defined. This activity is the responsibility of the users of the cadres. The final product is a 'qualification characteristic' which describes in detail what the training should achieve.

During the second stage, the evaluation strategy is formed, which gives an answer as to how, when and in what way it should be carried out. The most appropriate and effective combination of training methods, as well as the tools and means used for their implementation, are also determined.

During the third stage of the design, the main and the supporting objectives resulting from them are structured, as well as the main details in the training scope. This enables the training specification to be formed as a result of the output data from the analysis and scope [14, p. 38].

It is important to emphasize that the Guidance (JSP 822 V7.0) defines the design of training as the responsibility of

both the users of the cadres and the organization providing the training.

Guided by the above considerations, we must also emphasize the fact that when it comes to training officer-cadets at the NMU "V. Levski", additional emphasis should be placed on factors such as: training goals – they will be different from those valid for training servicemen from military units, as well as diversity in the homogenous target group – officer-cadets, but training in different specializations.

IV. CONCLUSIONS AND SUMMARY

Effective management of the military education system requires a structured and systematic approach to training, ensuring alignment with institutional goals and operational demands. The SAT provides a framework that enhances efficiency, coherence, and effectiveness in training design. Based on the theoretical and practical analysis of the training design phase, the following key conclusions can be drawn:

1. Alignment with training needs and resources. Training programs must be designed to meet the specific needs of trainees while efficiently utilizing available resources.

2. Coherence between content, structure, and objectives. The structure and content of training should be directly aligned with well-defined learning objectives, ensuring clarity in the expected outcomes.

3. Appropriate training methods and tools. The selection of teaching methods and tools should be tailored to the content and structure of the training, maximizing learning effectiveness.

4. Comprehensive assessment system. The evaluation of training outcomes must provide clear insights into whether trainees have successfully achieved the intended learning objectives.

The main advantages of the design phase, leading to structured learning, can be outlined in the following areas:

- Enables precise identification of training goals (at both individual and collective levels) and the most effective ways to achieve them;

- Ensures the selection of relevant learning materials aligned with training objectives;

- Establishes a direct correlation between evaluation methods and learning outcomes, improving assessment reliability and ensuring that the assessment accurately reflects the competencies acquired by the trainees;

- Adapts training strategies to both instructional styles and learner preferences, maximizing effectiveness.

Regardless of what training products the systems approach is applied to, and in particular the design phase, it allows training professionals to adopt a structured, methodical approach to planning the training activity. In the context of military educational institutions, the implementation of SAT will contribute to the design of training and the development of high-quality curricula that will increase the effectiveness of training, optimize the use of resources and ultimately provide better prepared officers for the evolving demands of modern military operations.

REFERENCES

[1] M. I. Popenţa, "Education-Training-Instruction" in the Romanian Army Commanding Officers Military Education. Conceptual Clarification," *Revista Academiei Forţelor Terestre*, no. 1 (73), pp. 17-22, 2014. [Online]. Available: https://www.armyacademy.ro/reviste/rev1_2014/POPENTA.pdf. [Accessed November 22, 2023].

[2] M. Armstrong, and S. Taylor, *Armstrong's Handbook of Human Resource Management Practice,* 13th ed. London: Kogan Page Limited, 2014. ISBN 978 0 7494 6964 1.

[3] Department of the Army Headquarters, *TRADOC Regulation 350-70, Army Learning Policy and Systems.* Fort Eustis, Virginia 23604-5700: United States Army Training and Doctrine Command, 2017. [Online]. Available: https://adminpubs.tradoc.army.mil/regulations/TR350-70.pdf. [Accessed November 27, 2023]..

[4] North Atlantic Military Committee, *MC 0458/4 – NATO Education, Training, Exercises and Evaluation (ETEE) Policy.* Brussels: NATO, 2023. [Online]. Available: https://www.coemed.org/files/Branches/DH/0458-4_20230103_NU_NATO_EDUCATION_TRAINING_EXERCISES_AND_EVALUATION_POLICY.pdf. [Accessed December 12, 2023].

[5] North Atlantic Military Committee, *MC 0458/3 – NATO Education, Training, Exercises and Evaluation (ETEE) Policy*. Brussels: NATO, 2014. [Online]. Available: https://www.coemed.org/files/Branches/DH/Files_01/MC0458-3-Final-NATO-EDUCATION,-TRAINING,-EXERCISES,-AND-EVALUATION-(ETEE)-POLICY-03-Sep-14.pdf. [Accessed December 12, 2023].

[6] Ministry of Defence, "Policy: JSP 822 Defence Training and Education V7.0 (Feb 24)," *Defence direction and guidance for training and education (JSP 822)*, vol. 1, p. 4, 8, 2024. [Online]. Available: https://assets.publishing.service.gov.uk/media/65ce3ea7e1bdec001132220d/JSP_822_V7.0__Vol_1_V3.0_-_Introduction.pdf. [Accessed March 27, 2024].

[7] M. Nachev, et al., *Doctrine for training the armed forces of the Republic of Bulgaria.* (National publication of the Armed Forces of the Republic of Bulgaria NP-7). Sofia: Ministry of Defense, 2012. [in Bulgarian].

[8] *The National Qualification Framework of the Republic of Bulgaria*, adopted by Decision of the Council of Ministers No. 96/02.02.2012. [in Bulgarian]. Available: https://www.navet.government.bg/bg/media/NQF_bg.pdf. [Accessed December 17, 2023].

[9] *Ordinance on the state requirements for the acquisition of higher education at the educational-qualification degree "bachelor" in the professional direction "Military Affairs" in the specialties of the regulated profession "officer for tactical management level"*. Adopted by Decree of the Council of Ministers No. 205 of 30.08.2012, in force from the academic year 2012 - 2013, Pron. DV. no. 68 of 4 September 2012, with final change and add. DV. No. 9 of January 26, 2018 [in Bulgarian]. Available: https://lex.bg/laws/ldoc/2135808720. [Accessed December 17, 2023].

[10] International Military Staff, *4th DRAFT MC 0458/2 – NATO Education, Training, Exercise and Evaluation (ETEE) Policy*. Brussels: NATO, 2009.

[11] Ministry of Defence, *JSP 822 Defence Direction and Guidance for Training and Education, Pt 2 (V3.0 Apr 17)*. London: Ministry of Defence, 2017.

[12] S. Dhawan, *The Systematic Approach to Training: Main Phases of the Training Cycle*. Course Hero, n.d. [Online, paywall]. Available: https://www.coursehero.com/file/71084086/Systematic-approach-to-trainingpdf/. [Accessed November 24, 2023].

[13] M. Hamza, *Developing Training Material Guide*. Karlstad: Swedish Civil Contingencies Agency (MSB), 2012. ISBN 978-91-7383-303-5. [Online]. Available: https://www.msb.se/siteassets/dokument/publikationer/english-publications/training-material-development-guide.pdf. [Accessed November 24, 2023].

[14] Ministry of Defence, "Policy: JSP 822 Defence Training and Education V7.0 (Feb 24)," *Defence direction and guidance for training and education (JSP 822)*, vol. 2, 2024. [Online]. Available: https://assets.publishing.service.gov.uk/media/65ce3ec80f4eb1001aa9811d/JSP_822_V7.0__Vol_2_V3.0_-_Defence_Individual_Training.pdf. [Accessed March 27, 2024].

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 69-72

The Role of Digitalization in the Fight Against Corruption

Jordan Deliversky
Department of National Security
University of Library Studies and
Information Technologies
Sofia, Bulgaria
j.deliversky@unibit.bg

***Abstract*—Digital technologies are becoming increasingly of main importance and provide a growing influence on public life. It impacts corruption and its counteraction across various sectors of society. At the current stage of society development, there are high expectations for combating this social phenomenon, and the advancement of information technologies and digitalization presents significant potential and prospects in the fight against corruption. This article examines possible trends and perspectives for utilizing digital tools in the fight against corruption, as well as identifying risks and new threats related to corruption in the context of digitalization processes in public administration and the digitization of services provided to citizens.**

***Keywords*—Corruption, digitalization, e-government, integrity.**

I. INTRODUCTION

In the modern digital age, the rapid advancement of technology has fundamentally reshaped the way public life operates, revolutionizing governance, public administration, and various social sectors. The integration of digital technologies such as artificial intelligence (AI), blockchain, big data analytics, cloud computing, and digital identity systems has not only streamlined public services but has also emerged as a powerful tool for enhancing transparency, improving efficiency, and mitigating corruption risks[1]. In particular, digital transformation has redefined how governments function, how public services are delivered, and how citizens interact with public and government institutions, creating an environment where oversight and accountability are significantly strengthened.

Corruption, long recognized as a major impediment to economic development and social justice, thrives in environments characterized by bureaucratic structures, excessive discretion in decision-making, limited access to information, and weak institutional controls. Traditionally, manual administrative processes, paper-based record-keeping, and face-to-face interactions in public service transactions have created opportunities for bribery, favoritism, fraud[2]. The absence of digital traceability in such systems has allowed corrupt practices to persist undetected, weakening public trust in institutions and impeding socioeconomic progress.

However, the increasing adoption of digital governance tools and automated decision-making systems has begun to dismantle these long-standing vulnerabilities by introducing greater transparency, reducing human discretion, and strengthening regulatory oversight[3]. For example, e-government platforms have digitized and centralized key public services such as tax collection, business registration, and social welfare distribution, significantly reducing opportunities for corrupt intermediaries to exploit bureaucratic inefficiencies. Likewise, blockchain technology is being leveraged to create immutable records of transactions in government procurement and public finance, ensuring that all transactions remain tamper-proof and fully auditable. Artificial intelligence and big data analytics are also playing a crucial role in corruption detection by analyzing patterns in financial transactions and flagging suspicious activities that may indicate fraudulent practices.

Moreover, open data initiatives and digital citizen engagement platforms have empowered civil society to participate more actively in governance, facilitating real-time monitoring of public spending and project implementation [4]. By making government contracts, budgets, and administrative decisions publicly accessible online, digital platforms enable journalists, non-governmental organizations (NGOs), and the general public to evaluate public sector activities, reducing opportunities for corruption to go unnoticed. Additionally, whistleblower protection mechanisms embedded in secure digital platforms allow individuals to report corruption

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8494
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

anonymously, providing a safer environment for exposing wrongdoing.

The influence of digital technologies extends beyond government operations, affecting key sectors of public life such as law enforcement, healthcare, education, and financial services. In law enforcement, digitalization has enhanced case tracking and forensic investigations, reducing opportunities for tampering with evidence or manipulating judicial processes. In healthcare, electronic health records (EHRs) and blockchain-based pharmaceutical supply chains ensure the integrity of medical procurement, preventing fraud and counterfeit drug circulation. The education sector benefits from digital transparency tools that prevent nepotism in faculty hiring, scholarship distribution, and academic assessments. Additionally, financial technology (FinTech) solutions such as digital payments and AI-driven fraud detection systems have curtailed money laundering and financial crimes, further limiting corruption opportunities in the banking sector.

Despite these promising developments, challenges remain in fully leveraging digital technologies to combat corruption. Cybersecurity threats, algorithmic biases, digital exclusion, and resistance from entrenched power structures pose significant hurdles to digital anti-corruption strategies. Governments must ensure that digital governance systems are inclusive, ethically designed, and resilient to cyberattacks to maximize their effectiveness in curbing corruption.

II. MATHERIALS AND METHODS

In the contemporary fight against corruption in the public sector, digitalization has emerged as a pivotal strategy, introducing tools and systems that enhance transparency, accountability, and efficiency. By integrating digital technologies into public administration, governments worldwide are addressing systemic vulnerabilities that have historically facilitated corrupt practices[5]. Some of the activities focus towards enhancing transparency and accountability, another refer to streamlining public services while other actions are facing towards goals on promoting of citizen engagement, as well as towards implementation of advanced monitoring tools for assuring, strengthening and guarding the integrity of public institutions.

Digital platforms enable the public to access government data, fostering an environment where information is open and verifiable. For instance, e-government initiatives provide citizens with insights into governmental operations, reducing the opacity that often conceals corrupt activities. The implementation of digital platforms in the public sector serves as a cornerstone for promoting transparency. By digitizing records and processes, governments can make vast amounts of data accessible to the public, including budgets, expenditures, procurement contracts, and policy decisions. This accessibility allows citizens, researchers, and organizations to follow government actions, identify discrepancies, and determine potential misconduct.

For instance, the Open Government Partnership (OGP) is a global initiative that encourages member countries to adopt transparent practices by leveraging digital technologies. Participating nations commit to making governmental data open and machine-readable, facilitating easier analysis and fostering public trust. Such initiatives underscore the role of digital platforms in transforming opaque governmental processes into transparent and accountable systems.

Other initiatives also have impact on corruption. E-government refers to the use of digital tools and systems to deliver governmental services, disseminate information, and facilitate interactions with citizens and businesses [6]. By transitioning from manual, paper-based processes to digital interfaces, e-government reduces opportunities for corruption in several ways. Some of them include process automation, transparent procurement, real-time monitoring.

Automating routine tasks minimizes human intervention, thereby reducing the chances of bribery and favoritism. For example, online licensing and permitting systems can eliminate the need for in-person interactions, where corrupt exchanges might occur.

Digital procurement platforms can publish all stages of the procurement process, from tender announcements to contract awards. This transparency deters collusion and bid-rigging by making the process open to public scrutiny.

E-government systems enable real-time tracking of public funds and projects. Citizens can monitor how their taxes are being utilized, which projects are being funded, and the progress of public works, thereby holding officials accountable for delays or mismanagement.

Empirical studies have demonstrated the effectiveness of digital platforms in combating public sector corruption. Research analyzing data from 110 countries between 2003 and 2021 found a significant negative correlation between the implementation of e-government initiatives and the prevalence of corruption. The study suggests that as governments adopt digital tools, the increased transparency and reduced human discretion lead to lower levels of corrupt activities [7].

Another study focusing on European countries during 2012–2019 corroborated these findings, indicating that e-government significantly curbs corruption by enhancing transparency and accountability in public administration. These studies provide robust scientific evidence that digital platforms and e-government initiatives are effective tools in the fight against public sector corruption [8].

The integration of digital platforms into governmental operations plays a crucial role in fostering transparency and reducing corruption. By providing public access to comprehensive and verifiable data, these platforms empower citizens to hold public officials accountable and deter misconduct. E-government initiatives, in particular, streamline processes, enhance openness, and diminish opportunities for corrupt practices. Scientific research supports the efficacy of these digital interventions,

highlighting their importance in promoting integrity and trust in public sector institutions.

Digital technologies have become essential in the global fight against corruption, offering innovative tools to detect, prevent and combat corruption practices across various sectors[9]. The mechanisms through which these technologies operate disrupt traditional avenues for corrupt practices and promote accountability.

In relation to enhancing transparency and accountability, open data policies are an important tool. Conducting and implementing such mechanisms into fight against corruption ensures that information related to government budgets, expenditures, procurement processes, and decision-making are actually available to the public[10]. The Open Data Charter's "Open Up Guide to Combat Corruption" identifies priority datasets and standards that governments can adopt to tackle corruption effectively.

Accessible government data allows stakeholders to hold public officials accountable for their actions. When data on public spending and procurement is open, it enables the detection of irregularities, such as inflated contracts or misallocation of funds[11].

While open data policies are instrumental in combating corruption, their success depends on several factors. For open data to be effective, it must be accurate, up-to-date, and comprehensive. Incomplete or outdated data can lead to misinformation and reduce trust in public institutions. Establishing robust legal frameworks is essential to mandate the release of government data and protect the rights of those who use it. Adequate infrastructure is necessary to collect, manage, and disseminate data efficiently. This includes investing in digital platforms and ensuring interoperability between systems. Another important factor is related to capacity building. Training public officials and citizens in data literacy ensures that data is both published effectively and utilized appropriately for monitoring and advocacy purposes [12].

III. Results and discussion

Digitalization offers promising tools to combat corruption, but there are various limitations and challenges which must be considered to ensure its effective implementation.

The success of digital transformation in anti-corruption efforts is heavily influenced by the existing institutional, social and political environment. Factors such as institutional incentives, state capacities, and leadership within the public sector play crucial role [13]. Without a conducive context, digital initiatives may face resistance or may not achieve the desired impact. The process of digital transformation itself can become a hotspot for corrupt activities if not managed carefully.

The procurement of digital systems, allocation of resources, and management of digital projects can be susceptible to corruption, undermining the very objectives of such initiatives. The effectiveness of digital anti-corruption tools is contingent upon adequate digital infrastructure and literacy. In regions where access to technology is limited, these tools may not reach or benefit the entire population, potentially exacerbating existing inequalities and leaving certain groups more vulnerable to corruption.

While digital tools can deter corruption, they can also be exploited for illicit purposes. Technologies such as cryptocurrencies and the dark web can facilitate anonymous transactions, making it challenging to trace illicit financial flows. Additionally, without proper safeguards, digital platforms intended for transparency can be manipulated to serve corrupt interests.

Bulgaria has been actively involved in blockchain-related activities, with several notable projects and incidents highlighting both the potential and challenges of using blockchain technology to combat corruption. In recent years, Bulgarian authorities have engaged in operations targeting fraudulent cryptocurrency schemes, underscoring the country's commitment to addressing financial crimes associated with digital assets. For instance, in January 2023, a coordinated action supported by Eurojust and Europol led to the dismantling of a cryptocurrency fraud network operating from Bulgaria, Cyprus, and Serbia[14]. This network had defrauded numerous victims across countries, including Germany, Switzerland, and Austria, through call centers promoting fake crypto investments. The operation resulted in multiple arrests and the seizure of significant assets, including over 150 computers and substantial amounts of cryptocurrency and cash.

While digitalization holds significant potential in the fight against corruption by enhancing transparency and accountability, it is not a panacea. The deployment of technologies like artificial intelligence in monitoring and data analysis also raises concerns about privacy and ethics[15]. There is a risk of excessive surveillance and potential violations of individual rights if these tools are not implemented with appropriate checks and balances. Only through comprehensive measures can digital tools effectively contribute to reducing corruption across various sectors.

IV. Conclusion

Digital technologies present a multifaceted approach to detecting and combating corruption by enhancing transparency, automating processes, enabling advanced analytics, and fostering citizen engagement. While challenges remain, strategic implementation and continuous oversight can harness the potential of these technologies to promote integrity and accountability across various sectors [16].

The integration of digital platforms into governmental operations plays a crucial role in fostering transparency and reducing corruption. By providing public access to comprehensive and verifiable data, these platforms empower citizens to hold public officials accountable and deter misconduct. E-government initiatives, in particular,

streamline processes, enhance openness, and diminish opportunities for corrupt practices.

Open data policies are a powerful tool in the fight against corruption. By fostering transparency, enhancing accountability, and enabling public scrutiny, these policies help to create an environment where corrupt practices are more easily detected and deterred. However, the successful implementation of open data initiatives requires careful consideration of data quality, legal frameworks, technological infrastructure, and capacity building to maximize their impact on reducing corruption.

REFERENCES

[1] J. C. Bertot, P. T. Jaeger, and J. M. Grimes, "Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools," Government Information Quarterly, vol. 27, no. 3, pp. 264–271, 2010. [Online]. [Accessed February 24, 2025] Available: https://doi.org/10.1016/j.giq.2010.03.001

[2] A. Persson, B. Rothstein, and J. Teorell, "Why anti-corruption reforms fail—Systemic corruption as a collective action problem," Governance, vol. 26, no. 3, pp. 449–471, 2013. [Online]. [Accessed February 24, 2025]Available: https://doi.org/10.1111/gove.12032

[3] D. C. Shim and T. H. Eom, "E-government and anti-corruption: Empirical analysis of international data," International Journal of Public Administration, vol. 31, no. 3, pp. 298–316, 2008. [Online]. [Accessed February 24, 2025] Available: https://doi.org/10.1080/01900690701590553

[4] M. Ramaswamy, "Using digital technologies to combat corruption in transition countries," Issues in Information Systems, vol. 25, no. 1, pp. 58–70, 2024. [Online]. [Accessed February 24, 2025] Available: https://iacis.org/iis/2024/1_iis_2024_58_70.pdf

[5] A. Mungiu-Pippidi and R. Dadašov, "When do anti-corruption laws matter? The evidence on public integrity enabling contexts," Crime, Law, and Social Change, vol. 68, no. 4, pp. 387–402, 2017. [Online]. [Accessed February 24, 2025] Available: https://doi.org/10.1007/s10611-017-9701-6

[6] S. Denchev, I. Peteva, and S. Yordanova, "Information literacy, information transparency, and information accessibility – Distinctive features of cyber security," in Proc. IMCIC - Int. Multi-Conf. Complexity, Informatics, and Cybernetics, vol. 2024-March, pp. 145–147, 2024. ISSN: 2771-5914, ISBN: 978-195049278-7. [Online]. [Accessed February 24, 2025] Available: https://doi.org/10.54808/IMCIC2024.01.145

[7] D. A. Seiam and D. Salman, "Examining the global influence of e-governance on corruption: A panel data analysis," Future Business Journal, vol. 10, p. 29, 2024. [Online]. [Accessed February 24, 2025] Available: https://doi.org/10.1186/s43093-024-00319-3

[8] L. T. Ha, T. T. To, T. T. Huyen, H. Q. Hoa, and T. A. Ngoc, "The roles of e-government in combating corruption: Evidence from European countries," Journal of Science and Technology Policy Management, vol. 15, no. 6, pp. 1505–1533, 2024. [Online]. [Accessed February 24, 2025] Available: https://doi.org/10.1108/JSTPM-04-2022-0065

[9] G. Dimitrov and M. Zahariev, Cyber Law in Bulgaria. The Netherlands: Kluwer Law International BV, 2024, 322 pages. ISBN: 978-94-035-4955-2.

[10] M. Zahariev, "Data protection aspects of artificial intelligence in commercial arbitration," Contemporary Strategies and Innovations in the Knowledge Management, ZA BUKVITE – O Pismeneh Publishing House, 2018, pp. 129–139. ISSN: 2535-0250.

[11] Council of Europe, "Enhancing the capacities of the Bulgarian Financial Intelligence on operational analysis," Council of Europe, 2024. [Online]. Available: https://www.coe.int/en/web/corruption/-/enhancing-the-capacities-of-the-bulgarian-financial-intelligence-on-operational-analysis[Accessed February 24, 2025]

[12] S. Denchev and T. Trencheva, "Model for cyber ethical and transparency issues in education: A short overview," in Proc. 15th Int. Technology, Education and Development Conf. (INTED 2021), Online Conf., 8-9 Mar. 2021, pp. 7583–7588. ISBN: 978-84-09-27666-0 / ISSN: 2340-1079. [Online]. [Accessed February 24, 2025] Available: https://doi.org/10.21125/inted.2021.1527

[13] D. Stoeva and A. Stoilov, "Trends in cyber threats - Problems and solutions," in Modern Dimensions in European Education and Research Area: Proc. 16th Int. Traveling Seminar of ULSIT, 2022, pp. 201–206. Academic Publisher "Za Bukvite – O Pismeneh." ISSN: 2367-7988.W.-K. Chen, Linear Networks and Systems. Belmont, CA: Wadsworth, 1993, pp. 123-135.

[14] European Union Agency for Criminal Justice Cooperation (Eurojust), "Takedown of fraudulent cryptocurrency network in Bulgaria, Cyprus, and Serbia," Press Release, 2023. [Online]. Available: https://www.eurojust.europa.eu/news/takedown-fraudulent-cryptocurrency-network-bulgaria-cyprus-and-serbia [Accessed February 24, 2025]

[15] M. Neykova, "Digitalization of registers in the public administration - Key element of electronic governance," Univ. Economics and Innovation in Lublin, Free Univ. Varna, ISSN: 2367-4555.

[16] M. Ivanova and G. Angelov, "Architectural approach to describe processes in CIS (communication information system) of organizational management structures," Education, Scientific Research and Innovations, vol. 1, no. 3, pp. 28–35, 2023.

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 73-80

Legal Aspects of European Union Armaments Cooperation: Challenges and Opportunities for Integration

Todor Dimitrov
Rakovski National Defence College
Sofia, Bulgaria
t.d.dimitrov@rndc.bg

***Abstract* — European armaments cooperation is governed by a complex legal framework, integrating international agreements, EU regulations, and national laws. Given the evolving geopolitical situation in Europe, marked by active and frozen conflicts near EU borders, the need for efficient and transparent legal mechanisms in defense cooperation has become more urgent. The paper explores the legal aspects of cooperative armament programs, assessing key regulatory challenges and institutional mechanisms, such as the European Defence Fund, Permanent Structured Cooperation, and the European Defence Agency. It examines the interplay between EU law and national sovereignty, focusing on Article 346 Treaty on the Functioning of the European Union and its implications for defense procurement and competition rules. By identifying legal uncertainties and proposing solutions to enhance transparency and effectiveness, the study highlights the necessity of legal harmonization to strengthen Europe's strategic autonomy and security resilience in the current geopolitical climate.**

Keywords* — *Armaments cooperation, Legal framework, European Union, Common Security and Defence Policy.

I. INTRODUCTION

The ongoing war in Ukraine and US President Donald Trump's call for European partners to increase their defense spending and contribution to security in Europe demonstrate the need to find approaches to achieving strategic autonomy in EU defense. Over the years, a number of successful European armaments cooperation (EAC) projects have been developed: Eurofighter Typhoon, FREMM (Fregata Europea Multi-Missione) program, Meteor Beyond Visual Range Air-to-Air Missile (BVRAAM), A400M Atlas, etc. These programs illustrate Europe's efforts to foster defense collaboration and technological innovation in armaments. In light of evolving security challenges and external pressures, many European nations reassessed and increased their defense budgets. Between 2021 and 2024, EU member states' total defense expenditure rose by more than 30%, reaching an estimated €326 billion in 2024. The growing trend of the last years was confirmed in 2024, when defence equipment procurement spending reached beyond €90 billion, with 88.2% of defence investments allocated to the procurement of new defence products [1]. The escalation in EU defense spending brings to the forefront critical legal considerations that must be addressed to enhance armaments cooperation. By adapting budgetary regulations, harmonizing procurement laws, and strengthening the overarching legal framework, the EU can foster a more integrated and resilient defense posture. In the context of evolving security challenges, huge defense expenditure, and the need for efficient defense capabilities EAC has become increasingly significant. Collaborative programs among European nations aim to enhance interoperability, reduce costs through economies of scale, and strengthen the European defense technological and industrial base (EDTIB). EAC is a cornerstone of the EU defense strategy, aiming to enhance military capabilities, bolster industrial competitiveness, and ensure strategic autonomy. However, these cooperative efforts are governed by a complex legal framework that encompasses international agreements, EU regulations, and national laws. This paper provides a comprehensive analysis of the legal aspects surrounding cooperative programmes in EAC, highlighting the challenges and proposing solutions to enhance legal clarity and effectiveness.

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8488
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

II. MATERIALS AND METODS

A. *International Legal Framework*

To effectively encompass the multilateral legal environment governing the EAC, it is necessary to analyse both international agreements and specific EU legal instruments. Firstly, we will consider international agreements. An international treaty is an agreement between subjects of international law, usually concluded in writing, regardless of its name and regardless of whether it consists of one or several related documents. The law of international treaties is a well-codified part of public international law. It also includes a significant number of specific international treaties, such as the founding acts of international organizations [2]. EU armaments cooperation is governed by a complex legal framework, integrating EU treaties and international agreements. The Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU) establish the foundation and legal principles for EU defense policy, while the Letter of Intent (LoI) Framework Agreement facilitates industrial collaboration.

The Treaty on European Union (TEU) defines the Common Foreign and Security Policy (CFSP) and the Common Security and Defence Policy (CSDP), outlining the EU's role in international peace and security. Articles 42 to 46 allow for the progressive framing of a common defense policy, enabling member states to undertake joint defense-related actions [3]. Permanent Structured Cooperation (PESCO), under Article 46, provides a framework for deeper collaboration among willing members. Despite these provisions, sovereignty concerns remain a challenge, as defense remains a sensitive national competency. Decision-making within CFSP and CSDP requires unanimous agreement, which can slow down cooperative initiatives.

The Treaty on the Functioning of the European Union (TFEU) complements the TEU by detailing EU competencies, including defense industry regulations. Article 346 TFEU allows member states to exempt defense contracts from standard procurement rules when essential security interests are at stake [4]. However, the European Court of Justice (ECJ) has ruled that this provision must be narrowly interpreted, limiting its misuse.

The Letter of Intent (LoI) Framework Agreement for European Defence Industrial Restructuration is a treaty signed by six European countries in 2000, and facilitates defense industry restructuring and collaboration. Its objectives include harmonizing regulations, promoting cross-border industrial cooperation, and strengthening the EDTIB. By addressing legal and administrative barriers, the LoI enhances multinational defense cooperation. However, the UK's departure from the EU raises questions about its future role. Additionally, aligning LoI provisions with EU policies, particularly in competition and procurement, remains a challenge. Although the LoI is intergovernmental, EU member states must ensure it complies with EU law, particularly in cases of conflict where EU law takes priority. The EU treaties provide a legal foundation for defense cooperation, balancing national sovereignty with collective objectives. The LoI complements this framework by fostering industrial cooperation, ensuring greater integration of European defense capabilities.

B. *European Union Legal Instruments*

When you search the term "armament" on official site of EU [5] you will find 1381 results. That mean almost 14 hundred documents related with it – Legal acts, Treaties, Law making procedures, International agreements, Case-law etc. This demonstrates that EAC operates within a complex legal framework, encompassing multiple EU legal instruments. These regulations facilitate collaboration, ensuring transparency, competition, and security while addressing challenges like national sovereignty and market fragmentation.

The Defence Procurement Directive (2009/81/EC), adopted in 2009, regulates procurement procedures for defense and sensitive security equipment, works, and services within the EU [6]. It harmonizes national procurement laws, enhances transparency, and opens the internal market for defense products while permitting exemptions to safeguard essential security interests under Article 346 TFEU. The Directive promotes fair competition by reducing legal barriers for cross-border cooperation among companies. However, differences in its interpretation and implementation may lead some states to favor national suppliers, limiting competition. Although exemptions are allowed, overreliance can undermine market objectives. The European Commission monitors the Directive's application and has initiated infringement proceedings against states that misuse exemptions. Additionally, ECJ rulings have clarified that any exemptions must be justified, proportionate, and narrowly interpreted, thereby establishing binding legal precedent for member states.

The Intra-Community Transfers Directive (2009/43/EC), adopted in 2009, simplifies the terms and conditions for the transfer of defense-related products within the EU [7]. It optimizes the transfer of defense-related products within the EU by harmonizing and simplifying licensing procedures. It aims to reduce administrative burdens, facilitate industrial cooperation, and support the integration of the European defense market, while ensuring that security remains uncompromised. The Directive introduces general transfer licenses, allowing specific defense products to move without individual licensing, and global licenses, enabling multiple transfers to designated recipients. A certification system ensures companies meet responsibility criteria to access general licenses, while member states must publish national licensing requirements and exchange certification data to enhance transparency. For cooperative programs, the Directive accelerates supply chains, reduces delays in defense projects, and promotes industrial collaboration by easing transfers between companies. However, inconsistent implementation among member states

weakens its effectiveness, and security concerns must be managed to prevent risks. Recognition of certifications also remains a challenge, as differing national standards hinder mutual acceptance and create regulatory obstacles.

The European Defence Fund (EDF), launched in 2017, is an EU initiative designed to support collaborative defense Research and Development (R&D) among member states. Under the Multiannual Financial Framework (MFF) 2021-2027, it has been allocated €16.4 billion to enhance innovation and competitiveness within the European defense industry [1, 8]. This allocation encompasses various programs, including the EDF, which has a budget of €9,5 billion for the same period. The EDF aims to promote cooperation, reduce duplication of efforts, and strengthen the EDTIB by fostering investment in joint defense capabilities. The EDF offers full grants for research projects and co-financing of up to 20% for prototype development. Eligible projects must include at least three entities from three member states, ensuring broad European participation. The fund is managed by the European Commission, which, in collaboration with member states, sets priorities and issues funding calls. For cooperative programs, the EDF reduces financial strain on member states, aligning national R&D priorities and integrating Small and Medium-sized enterprises (SMEs) into defense innovation. Despite this, many SMEs encounter difficulties in accessing EDF funding due to complex eligibility criteria, limited administrative capacity, and the dominance of major defense firms in consortium-building. This raises concerns about unequal participation and the risk of market concentration in a few industrially advanced Member States. However, complex administrative requirements make application and management time-consuming. State aid compliance, ensuring fair distribution among smaller member states, and balancing strategic autonomy with market openness remain key challenges in its implementation. Another EU legal instrument is the European Peace Facility (EPF), which is an off-budget funding mechanism established by the EU in March 2021 to enhance its capacity to prevent conflicts, build peace, and strengthen international security. With a financial ceiling of over €17 billion for the 2021-2027 period, the EPF enables the EU to finance actions with military and defense implications under the CFSP [9]. In the context of EAC programmes, the EPF plays a significant role by financing the provision of military equipment and support to partner countries. This includes the supply of lethal military equipment, marking a shift in the EU's approach to security assistance.

The European Defence Agency (EDA), established under Council Joint Action 2004/551/CFSP, facilitates defense cooperation within the EU [10]. Operating under the CSDP, it plays a key role in legal harmonization by supporting the standardization of defense procurement laws and developing common military requirements, certification frameworks, and legal templates for cooperative programs. The Agency significantly impacts multinational defense initiatives by coordinating collaborative projects, providing legal and administrative support, and assisting in accessing EU funding mechanisms such as the European Defence Fund (EDF). As a key institutional actor, the agency influences the creation, interpretation, and implementation of legal frameworks governing armaments cooperation. However, the EDA faces several legal challenges, like Intellectual Property Rights (IPR) management, that remains complex in multinational projects involving proprietary technologies. Also, compliance with EU competition law must balance market fairness with strategic cooperation. Additionally, the Agency must navigate responsibility allocation and dispute resolution in international projects. Export control and licensing harmonization also pose difficulties, as varying national regulations hinder seamless defense cooperation.

In addition to primary legal instruments, several other EU initiatives and regulations contribute to the legal framework governing European armaments cooperation. These instruments support defense collaboration by addressing procurement, investment, mobility, cybersecurity, and arms export controls.

Permanent Structured Cooperation (PESCO) was established under Article 46 of the Treaty on European Union (TEU) and enables willing and capable member states to deepen their defense cooperation [11]. Participating states make binding commitments to invest in defense capabilities and develop joint projects in areas such as armaments cooperation. PESCO enhances collaborative development and procurement but requires compliance with EU regulations and alignment with the European Defence Fund (EDF) to ensure effective coordination.

The Coordinated Annual Review on Defence (CARD) is a mechanism through which member states share information on defense spending and capabilities. It aims to identify opportunities for cooperation and reduce fragmentation and duplication in defense investments. Participation in CARD is voluntary, and while information sharing is encouraged, it must respect confidentiality and national security considerations [10].

The Action Plan on Military Mobility addresses legal and infrastructural barriers to the movement of military personnel and equipment within the EU [12]. Its legal measures include the harmonization of regulations and procedures, facilitating rapid deployment across borders. Cooperation with NATO and non-EU countries is also considered to ensure interoperability with broader security frameworks.

The Cyber Defence Policy Framework establishes guidelines for cyber defense cooperation among member states [13]. It includes legal considerations related to compliance with EU cybersecurity regulations and the protection of critical infrastructure. Given the increasing importance of cyber warfare, this framework seeks to enhance collective resilience against cyber threats targeting military and defense assets.

Beyond these instruments, several other EU legal measures shape armaments cooperation. EU Common Position 2008/944/CFSP establishes guidelines on arms export controls, ensuring that defense exports comply with international security and human rights standards. The European Defence Action Plan (EDAP) outlines strategies for strengthening the competitiveness of the European defense industry. Interpretative Communications from the European Commission provide guidance on defense procurement and the application of Article 346 TFEU, clarifying the conditions under which exemptions from internal market rules are justified. Additionally, the Guidelines on State Aid for Defense establish rules for government support in the defense sector, ensuring compliance with EU competition law while promoting strategic investments in military capabilities. Ensuring the balance between national security and internal market rules remains a legal and political challenge.

C. NATO and EU Armaments cooperation

European armaments cooperation extends beyond the European Union (EU), involving partnerships with non-EU countries, primarily through NATO. As of 2025, NATO consists of 32 member states, including 30 European nations and 23 EU members, fostering interoperability, standardization, and collective defense capabilities. A key element in this collaboration is the implementation of NATO Standardization Agreements (STANAGs), which establish common military procedures and standards [14]. NATO influences European defense coordination by ensuring compatibility and efficiency in joint operations. The North Atlantic Treaty defines NATO's security principles, while Article 5 enshrines collective defense, treating an attack on one member as an attack on all. NATO also facilitates joint training, defense planning, and technological advancements. Cooperation with non-EU members, such as the United States, Canada, Turkey, Norway, and the United Kingdom, remains vital for European security. The NATO Status of Forces Agreement (SOFA) regulates legal protections and operational clarity, while the Partnership for Peace (PfP) Framework enables non-NATO states to engage in military collaboration. STANAGs ensure interoperability by aligning equipment, logistics, and operational strategies across NATO allies. Covering communications, logistics, medical support, and weapons systems, they promote joint procurement and defense standardization. While not legally binding unless integrated into national legislation, STANAGs play a crucial role in harmonizing procurement policies and ensuring compliance with EU defense regulations, particularly the Defence Procurement Directive. Legal challenges arise due to varying national legal frameworks, complicating uniform STANAG adoption. IPR must be clearly defined in joint development agreements, and technology transfers must comply with export control laws to prevent unauthorized distribution. Next, Legal responsibility in cooperative defense programs is another issue, as liability and dispute resolution mechanisms remain subject to national laws rather than a unified NATO legal system. Furthermore, Brexit also complicates NATO-EU defense relations. While the UK remains a NATO member, its exit from the EU requires new legal arrangements to maintain defense cooperation. STANAGs provide a framework for continued UK participation in European defense initiatives, ensuring compatibility with EU forces. However, the UK must balance NATO commitments while renegotiating its defense agreements with the EU.

D. National Legal considerations

European armaments cooperation operates within a complex legal framework, integrating international agreements, EU regulations, and national laws. While EU treaties and directives establish the foundation for collaboration, national legal considerations significantly impact the implementation of cooperative defense programs. Key areas influenced by national laws include sovereignty and national security, Article 346 TFEU exemptions, export controls, procurement regulations, IPR, and dispute resolution mechanisms.

Firstly, defense and national security are core elements of state sovereignty, granting EU member states full control over their defense policies, military capabilities, and defense industries [15]. Many nations have constitutional provisions or national laws prioritizing security interests, ensuring strategic autonomy in defense matters. Sovereignty concerns often lead to unwillingness in fully integrating defense industries or sharing sensitive technologies. Divergent threat perceptions among EU states shape their willingness to engage in cooperative programs, as national security priorities vary based on geopolitical factors. While the EU promotes deeper defense integration, states must balance collective security objectives with national sovereignty, creating challenges in harmonizing policies across the Union.

Next, Article 346 of the Treaty on the Functioning of the European Union (TFEU) allows member states to exempt defense contracts from standard EU procurement rules when essential security interests are at stake. However, its application must be justified, necessary, and proportionate, as excessive reliance on exemptions can hinder the EU's goal of an integrated defense market. Legal uncertainties surrounding Article 346 create obstacles to cooperation, as unclear obligations may deter potential partners. Overuse of exemptions fragments the market, reduces efficiency, and increases duplication in defense procurement. The European Court of Justice (ECJ) has ruled in cases like Commission v. Spain (C-414/97) that Article 346 should be narrowly interpreted, setting limits on its application. Different EU states apply Article 346 inconsistently. Germany has used it for strategic defense programs but has faced scrutiny. France invokes it for high-tech and nuclear programs while balancing EU obligations. However, divergent interpretations of "essential security interests" create legal inconsistencies and transparency challenges across the EU.

As regards Export Controls and Licensing, each EU member state regulates the export of military and dual-use goods through its national laws, maintaining sovereign control over defense exports. These laws are shaped by international agreements, such as the Wassenaar Arrangement and the Missile Technology Control Regime (MTCR), which establish global arms export standards. Differences in national export controls create legal complexities and delays in technology trasnsfers within cooperative defense programs. Export policies toward non-EU countries further complicate joint projects, as some states impose stricter controls. For instance, post-Brexit, the UK enforces an independent export control system, affecting its EU partnerships, while Sweden applies strict human rights-based restrictions, limiting participation in some joint programs. Efforts to harmonize export controls within the EU include the Intra-Community Transfers Directive (2009/43/EC) which aims to harmonize arms transfers within the EU, but inconsistent national implementation remains a challenge [7]. Balancing security interests with industrial competitiveness is crucial, as strict controls enhance security but may restrict market opportunities for defense manufacturers.

In addition, each EU member state follows distinct defense procurement policies, varying in procedures, evaluation criteria, and transparency standards. National laws governing defense contracts often include mechanisms like offset agreements and industrial participation requirements, favoring domestic industries. While these policies support national defense sectors, they also create barriers to cross-border cooperation. Ensuring legal compliance with EU directives and international agreements remains a challenge. Companies operating across multiple states face administrative burdens, higher costs, and procurement delays due to varying national requirements. Aligning national and EU regulations demands careful legal coordination, as inconsistencies hinder joint procurement efforts and defense market integration.

Furthermore, National laws regulate Intellectual Property Rights, including patents, trademarks, and trade secrets, which are essential in defense cooperation, particularly in R&D and technology-sharing agreements. However, variations in IPR protection across EU member states create legal uncertainties, affecting joint defense projects and shared technology development. Effective IPR management requires clear agreements on ownership, licensing, and access rights for jointly developed technologies. Without a harmonized framework, disputes over usage rights and royalties may arise, complicating defense collaboration. Different EU countries approach IPR protection differently. France enforces strict national control over defense innovations, while Spain supports collaborative R&D but applies specific registration rules. These differences highlight the need for standardized legal frameworks to facilitate cooperation while protecting proprietary technologies. Another challenge is confidentiality obligations. Protecting sensitive military research from unauthorized access must be balanced with transparency in cooperation, making IPR management a key legal issue in European armaments programs.

Moreover, National legal systems establish responsibility in defense contracts through contractual responsibility and tort law. Contractual responsibility defines liability for breaches, performance failures, and damages, while tort law covers non-contractual liability, such as negligence or product defects in defense manufacturing. In multinational defense programs, legal uncertainty arises due to differing national laws, complicating liability, contract enforcement, and performance disputes. This legal uncertainty stems primarily from the fragmentation of national legal standards regarding liability, the use of Article 346 TFEU to bypass EU procurement rules, and the absence of harmonised enforcement mechanisms for multinational contracts. Defense contracts must include choice of law and forum selection clauses to ensure disputes are resolved under a unified legal framework. Arbitration is often the preferred method for international dispute resolution, offering neutral venues and standardized procedures. Litigation in national courts raises concerns over impartiality and jurisdictional conflicts, while enforcing judgments across multiple jurisdictions remains a challenge. Sovereign immunity further complicates liability, as some states limit legal actions against government entities, making it difficult for contractors and partners to seek redress. Standardized legal frameworks addressing responsibility, liability, and dispute resolution are crucial for building trust and ensuring the efficiency of cooperative defense programs.

III. Results and Discussion

A. *Legal challenges in EAC*

Cooperative programmes in European armaments cooperation are essential for enhancing defense capabilities, promoting interoperability, and strengthening the EDTIB. However, these programmes face numerous legal challenges that can hinder their effectiveness. Some of the key legal challenges associated with cooperative armaments programmes in Europe include IPR management, competition law and antitrust issues, responsibility and dispute resolution mechanisms, export controls and third-country participation, divergent national legal frameworks, procurement and contractual complexities, standardization and interoperability, security of supply and classified information, and state aid and funding regulations.

Effective IPR management is essential in cooperative defense programs, where multiple nations contribute to research, development, and production. Legal uncertainties regarding ownership, licensing, and technology sharing can hinder collaboration. Clear IPR agreements specifying ownership structures, licensing terms, and dispute resolution mechanisms help mitigate these challenges. Harmonizing IPR policies across participating nations reduces legal inconsistencies and

enhances cooperation. Existing frameworks, such as the Organisation for Joint Armament Cooperation (OCCAR) IPR policy, offer guidelines for managing intellectual property in multinational defense programs, ensuring legal certainty.

European competition law prevents anti-competitive practices and ensures fairness in the defense sector. However, cooperative armaments programs require balancing security concerns with legal restrictions, as exclusivity agreements and industrial cooperation are often necessary. Early engagement with competition authorities helps clarify acceptable practices and prevent violations. Thorough legal assessments ensure compliance with EU and national laws, while in some cases, security needs justify exemptions, allowing defense cooperation without breaching antitrust regulations.

Establishing clear responsibility arrangements and dispute resolution mechanisms is crucial in managing risks associated with cooperative defense programs. Contracts should specify responsibilities, liability limitations, and indemnities, while defining applicable law and dispute resolution forums to prevent jurisdictional conflicts. International arbitration, under institutions like the International Chamber of Commerce (ICC) or the London Court of International Arbitration (LCIA), is often preferred for impartial resolutions. In some cases, governments may grant limited waivers of sovereign immunity to ensure legal accountability in cooperative agreements.

Export control regulations pose significant legal challenges in cooperative armaments programs, particularly when they involve third-country participation. Divergent national policies create uncertainties and delays in technology transfers. Early identification of export control issues helps develop compliance strategies, while harmonizing policies reduces inconsistencies and simplifies licensing. Organizations must implement strong compliance programs to meet national and international legal requirements effectively.

Challenges in aligning international agreements, EU instruments, and national laws persist in defense cooperation. Efforts to harmonize national defense laws within the EU face resistance due to sovereignty concerns, as member states prioritize national control over defense regulations. The EDA promotes legal standardization but lacks binding authority over national laws. Balancing national autonomy with EU integration remains a key issue. While the EU seeks greater efficiency and strategic autonomy, states continue to prioritize national security and industrial interests. Operating across multiple legal systems adds administrative burdens, requiring specialized legal expertise to navigate complex regulations effectively. Variations in national legal frameworks complicate cooperative defense projects, as each country follows distinct procurement, technology transfer, and security regulations. Developing unified legal frameworks, such as common contractual templates, can reduce inconsistencies. Aligning national laws with EU directives and international standards enhances legal harmonization, while legal experts help navigate multi-jurisdictional complexities.

Cooperative armaments programs face legal challenges due to differences in national procurement laws. Establishing joint procurement entities, such as OCCAR, centralizes processes and ensures compliance with EU regulations. Standardized procurement procedures improve transparency and efficiency, while open communication and transparent negotiations help secure agreements on contractual and financial obligations.

Regarding Standardization and Interoperability, one of the key challenges in cooperative armaments programs is ensuring that different national defense systems and technologies are compatible. Lack of standardization can reduce efficiency and create technical complications. To address this, programs should adopt common standards like NATO STANAGs or European defense standards to align requirements. Mutual recognition agreements for certifications and approvals can ease integration, while early coordination in development ensures that specifications meet the needs of all participating nations.

Security of supply and the protection of classified information present significant legal and strategic challenges in cooperative defense programs. Ensuring a stable supply chain for critical military equipment requires legal agreements that define security protocols and supply guarantees. International security agreements should be established to regulate the handling and sharing of classified information between program participants, ensuring that sensitive data remains protected. Legal safeguards must also be in place to enforce compliance with security requirements, particularly when dealing with defense-related intellectual property or proprietary technologies. Contracts should include provisions that secure alternative sources of supply to mitigate risks associated with political or economic disruptions.

EU state aid rules prevent market distortions but pose challenges for defense projects requiring public investment. Governments supporting national defense companies must navigate state aid regulations carefully. To ensure compliance, exemptions for defense-related projects must be properly applied. Cooperative programs should adopt structured funding mechanisms aligned with EDF requirements, ensuring EU regulation compliance. Engaging legal experts early in funding negotiations helps prevent legal infringements and ensures financial assistance remains sound.

B. Proposed solutions and recommendations for future integration

European armaments cooperation strengthens defense capabilities and supports strategic autonomy but faces legal challenges due to divergent national laws, complex EU regulations, and sovereignty concerns. Overcoming these obstacles requires legal harmonization, streamlined procurement rules, and structured collaboration

frameworks to ensure effective and legally sound cooperative programs.

a) Harmonization of Regulations

Improving armaments cooperation requires harmonizing regulations across EU member states. Efforts should focus on aligning key legal areas, fostering trust among stakeholders, and demonstrating the benefits of harmonization. The EU can provide financial and technical support, including through the European Defence Fund (EDF). Creating forums for legal experts and policymakers facilitates dialogue, addresses concerns, and ensures that harmonization efforts align with practical defense needs.

b) Clear Contractual Agreements

Standardized contractual frameworks are crucial for avoiding legal disputes and ensuring effective collaboration. Developing contract templates for defense cooperation can integrate best practices from previous programs. Engaging experienced legal professionals helps draft agreements that address the complexities of multinational defense projects. Early legal issue resolution prevents misunderstandings, aligns expectations, and establishes clear obligations for all parties.

c) Strengthening EU Legal Instruments

Enhancing existing EU directives and regulations can address current legal gaps and adapt to the evolving nature of defense technologies and cooperation. The European Commission and Parliament should prioritize legal reforms, engaging stakeholders to ensure practicality. Strengthening compliance monitoring and taking corrective actions will maintain legal integrity and build trust among member states. Additionally, involving industry representatives, national governments, and legal experts in the legislative process can ensure that new regulations are realistic and responsive to the defense sector's needs.

d) Enhanced Legal Support

Legal support is vital for successful defense cooperation. Adequate resources should be allocated to legal advisory services to assist with compliance, dispute resolution, and contractual obligations. Establishing online platforms and helpdesks can simplify legal navigation for participants. Collaboration with defense law professionals strengthens the legal framework, ensuring projects comply with EU and national regulations.

e) Strengthening International Cooperation

Legal cooperation between the EU and international organizations, including NATO and non-EU defense partners, is essential for ensuring compatibility in multinational defense projects. Establishing formal mechanisms for legal alignment can reduce regulatory conflicts. Policies that allow non-EU countries to participate in EU defense initiatives, while balancing openness and security, can enhance European security. Additionally, promoting the exchange of legal expertise and best practices at international forums and conferences can enhance understanding and improve legal interoperability among defense partners.

f) Addressing National Legal Challenges

Many legal barriers to EAC originate from national laws that are not fully aligned with EU defense objectives. Legal barriers often stem from national laws misaligned with EU defense objectives. Encouraging member states to review and amend restrictive laws, possibly through national action plans, can improve cooperation. The EU can provide technical assistance and guidelines to help align legal frameworks with common defense goals. Open communication between national governments and EU institutions is essential, while monitoring mechanisms can track legal reforms and ensure progress toward greater legal alignment.

g) Promoting Mutual Trust and Confidence

Mutual trust among member states is fundamental to the success of cooperative defense programs. Regular meetings among legal and defense officials can facilitate discussions on challenges and solutions. Joint initiatives, such as pilot projects and multinational defense research, can showcase the benefits of collaboration. Raising awareness of different legal systems fosters better communication, reducing misunderstandings in multinational agreements.

IV. CONCLUSION

European armaments cooperation is vital for strengthening defense capabilities and ensuring strategic autonomy. However, legal complexities, including divergent national laws, EU regulations, sovereignty concerns, and procurement challenges, continue to hinder efficient collaboration. Key legal obstacles such as IPR, export controls, competition law, and national procurement policies create fragmentation and inefficiencies in multinational defense projects. To address these issues, harmonization of regulations, standardized contractual agreements, stronger legal mechanisms, and enhanced NATO integration are necessary. Strengthening PESCO, the EDF, and the EDA, alongside improving dispute resolution, compliance monitoring, and mutual recognition of standards, can facilitate smoother cooperation. Success in European defense cooperation depends on legal clarity, trust, and strategic coordination. By fostering greater legal alignment and collaboration, Europe can enhance its collective defense capabilities, streamline joint armaments projects, and establish a more secure, efficient, and autonomous defense framework.

ACKNOWLEDGEMENT

The work was supported by Ministry of Education and Science in implementation of the National Strategy for the Development of Scientific Research 2017 - 2030 under the National Scientific Programme "Security and Defence", adopted by Decision of the Council of Ministers No 731 of 21 October 2021.

REFERENCES

[1] Council of the European Union, EU defence in numbers, Jan 28 2025, [Online], Available: https://www.consilium.europa.eu/en/policies/defence-numbers/, [Accessed: Jan 15, 2025]

[2] N. Nedev, Essence and Significance of Custom as a Source of International Humanitarian Law in the Context of Modern Armed Conflicts. Proceedings of Jubilee Scientific Conference 30 Years of the Faculty of National Security and Defense 1994 – 2024, Rakovski NDC, pp. 61-62 (2024) ISBN 978-619-7711-60-8

[3] The Treaty on European Union (TEU), Title V, Chapter 2, Section 2 - Provisions on the Common Security And Defence Policy, Official Journal of the European Union, C 202/1, Jun 7, 2016, [Online], Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12016ME/TXT, [Accessed: Jan 15, 2025]

[4] The Treaty on the Functioning of the European Union (TFEU), Article 346, Official Journal of the European Union, C 202/1, Jun 7, 2016, [Online], Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12016ME/ TXT, [Accessed: Jan 15, 2025]

[5] UK Ministry of Defence, Letter of Intent: restructuring the European defence industry, 4 August 2015, Available: https://www.gov.uk/guidance/letter-of-intent-restructuring-the-european-defence-industry, [Accessed: Jan 16, 2025]

[6] European parlament, EUR-Lex, [Online], Available: https://eur-lex.europa.eu/homepage.html, [Accessed: Jan 16, 2025]

[7] Defence Procurement Directive (2009/81/EC), Official Journal of the European Union, L 216/76, Aug 20, 2009, [Online], Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0081&qid=1740349791434, [Accessed: Jan 17, 2025]

[8] Intra-Community Transfers Directive (2009/43/EC), Official Journal of the European Union, L 146/1, Jun 10, 2009, [Online], Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0043&qid=1740350192929, [Accessed: Jan 17, 2025]

[9] European commission, The European Defence Fund at a glance, [Online], Available: https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en, [Accessed: Jan 21, 2025]

[10] European commission, European Peace Facility, [Online], Available: https://fpi.ec.europa.eu/what-we-do/european-peace-facility_en, [Accessed: Jan 21, 2025]

[11] European Defence Agency, [Online], Available: https://eda.europa.eu/, [Accessed: Jan 22, 2025]

[12] Permanent Structured Cooperation (PESCO), [Online], Available: www.pesco.europa.eu, [Accessed: Jan 22, 2025]

[13] European commission, Action plan on military mobility 2.0, Brussels, Nov 10, 2022, JOIN(2022) 48 final, [Online], Available: https://defence-industry-space.ec.europa.eu/system /files/2022-11, [Accessed: Jan 23, 2025]

[14] Council of the European Union, The European Cyber Defence Policy, Nov 10,.2022, [Online], Available: https://www.european-cyber-defence-policy.com/, [Accessed: Jan 23, 2025]

[15] NATO, Standardization, Oct 14, 2022, Available: https://www.nato.int/cps/cn/natohq/topics_69269.htm, [Accessed: Jan 24, 2025]

[16] C. Mölling, Sovereign, Capable, Innovative, Responsive: Prospects and challengesfor EU security and defence policy in the 10th parliamentary term, July 2024, Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/754457/EXPO_BRI(2024)754457_EN.pdf, [Accessed: Jan 24, 2025]

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 81-87

Radioactive Waste Storage as an Element of National Security

Nikolay Todorov Dolchinkov
Vasil Levski National Military University, Veliko Tarnovo, Bulgaria
Veliko Tarnovo, Bulgaria
n_dolchinkov@abv.bg

Nikolay Iliyanov Padarev
Vasil Levski National Military University, Veliko Tarnovo, Bulgaria
Veliko Tarnovo, Bulgaria
nikolai_padarev@abv.bg

***Abstract*— The presence of numerous nuclear power plants on the European continent is a guarantee of the energy security of the countries of the continent. At the same time, the problem of storing spent nuclear fuel is also deepening, because fewer and fewer manufacturers are engaged in its processing. The use of radioactive isotopes in medical diagnostics and treatment is also increasing, as well as in many sectors of the economy. But for now, the problem of storing these radioactive materials is lagging. The prospects for storing these materials have been examined and based on the data on the presence of radioactive waste, a systematic proposal for short-term and long-term storage of these materials has been made. The study is in its initial phase and the values are yet to be specified and a more precise proposal for storing nuclear waste is to be made.**

Keywords*— *medical diagnostics, medical treatment, national security, nuclear fuel, nuclear power plant, pollution, radioactive waste repository, radioactive isotope, storage.

I. Introduction

Nuclear waste storage is an important and complex issue related to the safety and sustainability of nuclear energy. Radioactive waste requires special storage conditions, as it remains hazardous to the environment and human health for thousands of years [1], [2].

One approach is the construction of deep geological repositories, which are located hundreds of meters below the earth's surface. In them, the waste is stored in special containers that are resistant to corrosion and mechanical damage. In Bulgaria, the construction of such a repository is planned by 2050, but a specific location has not yet been selected.

This process requires careful planning and public consent, as people often express concerns about the safety of such facilities [3], [4].

Nuclear waste is material that remains radioactive and hazardous after its use in nuclear technologies. It is usually classified into three categories:

1. Low-level waste - includes contaminated instruments, clothing and filters, which have relatively low levels of radiation.

2. Intermediate-level waste - usually includes materials from structures and equipment that have been exposed to radiation.

3. High-level waste – the most dangerous form, containing spent nuclear fuel and residues from nuclear reactions [5].

Who generates nuclear waste?

NPP (nuclear power plants): the main source of nuclear waste from electricity generation.

1. Medical industry: when using radioactive isotopes for diagnosis and treatment.

2. Scientific research: in laboratories working with radioactive substances.

3. Industry: when using radioactive materials for certain technological processes, such as quality control.

4. Military industry: in the production and maintenance of nuclear weapons.

Nuclear waste poses a major challenge for storage and management due to its long radioactivity period.

II. Materials and Methods

Nuclear waste management involves various approaches aimed at safe storage, reducing radiation hazards, and minimizing long-term risks [6], [7]. Here are the main methods:

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8502
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

Interim storage: The waste is initially stored in specially designed containers, usually on the site of the nuclear power plant. This is an interim step until a decision is made on long-term storage.

Long-term storage in geological repositories: Radioactive materials are isolated at great depth in stable geological formations [8]. This is considered one of the safest methods because it minimizes the impact on the environment and people.

Recycling and reuse: Spent nuclear fuel can be reprocessed to extract valuable materials, such as uranium and plutonium. This process reduces the amount of high-level waste.

Stabilization and encapsulation: The waste is treated chemically or physically to make it more stable before being encapsulated in durable containers.

Transmutation: An advanced method in which radioactive isotopes are converted into less radioactive ones through nuclear reactions. It is still under development and is not widely available.

Dry storage: Used for spent fuel that is cooled in special containers made of metal and concrete.

These methods are combined with strict regulations and monitoring to ensure maximum safety.

International standards for nuclear waste management have been established to ensure the safety of people and the environment. They include principles, guidelines, and regulations that are applied in different countries. Here are some key aspects:

- International Atomic Energy Agency (IAEA): The IAEA provides guidelines and standards for the safe management of radioactive waste, including storage, transportation, and disposal. A key document is the "Basic Principles for Radioactive Waste Management," which emphasizes the importance of long-term safety.
- European standards: Within the European Union, Directive 2011/70/Euratom establishes a framework for the responsible and safe management of spent fuel and radioactive waste. This directive requires Member States to develop national waste management programmes and ensure transparency.
- International conventions: The Convention on the Safety of Spent Fuel and Radioactive Waste Management is a key international treaty that promotes cooperation between States. The Convention on the Physical Protection of Nuclear Material also plays an important role in preventing unlawful access and use.
- National programmes: Each State is responsible for developing national programmes that meet international standards and take into account the specific conditions of the State [9], [10].

Improper storage of nuclear waste can have serious consequences for both the environment and human health. Here are some of the main risks:

- Environmental contamination: Radioactive substances can enter the soil, water sources and the atmosphere. This contamination can have long-term effects on ecosystems, destroying local flora and fauna.
- Human health hazards: Exposure to radiation can cause serious illnesses, including cancer, mutations and damage to the reproductive system. Even low levels of radiation can have a cumulative effect on human health.
- Accidents and incidents: Improper storage can lead to explosions, leaks or fires that can spread radioactivity over a wide radius. For example, the Chernobyl and Fukushima incidents have shown the catastrophic potential of such situations.
- Economic consequences: Contamination by radioactive waste can require enormous resources for clean-up and restoration. Affected regions often experience economic losses, such as loss of tourism and productivity.
- Social and political tensions: People living near poorly managed facilities may be forced to evacuate or suffer social stress. Such cases often trigger public protests and international criticism [1], [11], [12].

Proper management and storage are critical to minimizing these risks. The long-term effects of improper storage of nuclear waste can be catastrophic for nature, human health, and socio-economic development. Here is what can happen:

1. Persistent contamination of soil and water: Radioactive materials can leach into soil and water sources, causing contamination for hundreds or even thousands of years. This makes these resources unfit for use by humans, animals, and plants.

2. Genetic mutations and diseases: Long-term radiation can lead to genetic changes and serious health problems for generations to come. Common consequences include cancer, infertility, and hereditary diseases.

3. Destruction of ecosystems: Radioactivity can destroy biodiversity by killing plant and animal species or altering their natural habitat.

4. Economic and social challenges: The affected areas often remain uninhabited, leading to depopulation and loss of economic potential. Evacuation of the population and long-term clean-up require enormous resources.

5. Destabilization of public trust: Such situations can cause distrust in institutions and public tension.

Historical examples, such as the Chernobyl accident, show how improper management of radioactive substances can leave lasting scars on humanity and the planet. Proper

planning and strict regulations are key to preventing these dangers [13].

The short-term effects of improper storage of radioactive waste can be presented as:

1. Environmental contamination: Radioactive leaks can quickly spread into the soil, air and water, causing harm to local ecosystems.

2. Danger to humans and animals: Radiation emissions can expose humans and animals to radiation, leading to acute health problems such as radiation burns or poisoning.

3. Fires and explosions: Under unsafe conditions, radioactive materials can be a factor in accidents such as fires or explosions, which significantly increase the risk.

4. Social tensions: Lack of trust and panic can arise among the local population, especially if the problems are not well communicated [14].

Measures for proper storage of radioactive waste:

1. Use of specialized containers: Storage in resistant containers that protect against corrosion, leakage and mechanical damage.

2. Controlled repositories: Temporary storage in secure facilities that are well isolated and under strict monitoring.

3. Geological repositories: Long-term storage in stable geological formations where the waste is physically isolated.

4. Regular monitoring and inspections: Systematic monitoring and maintenance of facilities to prevent accidents.

5. Reprocessing and recycling: Reusing spent nuclear fuel to reduce the amount of radioactive waste.

6. Public awareness: Transparency in communication with the public to reduce fear and ensure support for projects.

These measures are critical to preventing the risks associated with radioactive waste [15], [16].

III. Results and discussion

Detecting improperly stored radioactive waste requires a combination of classical methods and modern technologies. Here are some of the traditional approaches and potential innovations in this field:

Classical methods

1. Geiger-Muller counter: One of the most well-known instruments for detecting radiation. It measures beta and gamma radiation and is used to scan suspicious locations.

2. Scintillation detectors: Used to measure radiation emissions by analysing the light emitted when radiation interacts with certain materials.

3. Soil and water sampling: Laboratory analysis of samples from contaminated areas can detect the presence of radioactive substances.

4. Handheld detectors: Portable devices that are used to inspect small areas or containers.

Modern and innovative methods

1. Drones with radiation sensors: Drones equipped with radiation detectors can scan large areas that are otherwise difficult for humans to access.

2. Spectroscopy: Advanced analysis that identifies specific radioactive isotopes by measuring the energy of their emission.

3. Satellite monitoring: Satellites with radiation sensors can locate areas of increased radiation over a large area.

4. Thermal infrared technology: Useful for detecting temperature anomalies that may indicate improperly stored radioactive waste.

5. Autonomous robots: Robots that can operate in hazardous areas and collect data without risk to humans.

6. Biological indicators: Monitoring changes in vegetation, animals, or microbes in areas can provide an indication of radioactive contamination.

The integration of classical and modern methods increases the effectiveness of hazard localization.

Preventive measures

1. Monitoring of risk areas: Continuous monitoring of areas with known nuclear activity.

2. Public awareness: Training the local population to recognize suspicious materials.

3. Regulatory inspections: Regular inspections of industrial and medical facilities.

These methods, combined with adequate training and technology, significantly assist in the detection and management of accidental radioactive waste [17].

High-level radioactive waste is stored using specialized methods that ensure safety and minimize risks to the environment and people. Here is how it is stored:

Nuclear waste storage methods can be categorized into the following types:

- Cooling pools: Spent nuclear fuel is initially stored in water pools that cool the fuel and provide radiation protection.
- Dry storage: After cooling, the fuel is transferred to special containers made of durable materials such as concrete and metal.
- Geological repositories: Long-term storage in stable geological formations that isolate radioactive materials from the environment.

In Bulgaria, spent nuclear fuel from the Kozloduy NPP is stored in specially constructed facilities. There is a dry storage facility on the plant site that ensures safety through the use of durable containers. In the past, the fuel was

returned to Russia for reprocessing, but now solutions are being sought for long-term storage in the country [18].

The government is considering the possibility of building a geological repository for long-term storage, but choosing a suitable location and public acceptance remain challenges [4].

In Bulgaria, the management of spent nuclear fuel (SNF) and high-level radioactive waste is a complex process that involves several stages and strategies for long-term storage. Here is more detailed information:

Current status of storage in Bulgaria

1. Interim storage:

Spent nuclear fuel from Kozloduy NPP is initially stored in near-reactor cooling pools. This is a standard practice that ensures safety and reduces the temperature of the fuel.

After cooling, the fuel is transferred to specially constructed dry storage facilities. In Bulgaria, CONSTOR 440 containers are used, which are resistant to corrosion and mechanical damage.

2. Long-term plans:

Bulgaria has the capacity to store SNF until 2032, but strategies for a longer-term solution are being worked on.

The possibility of building a geological repository is under discussion, but no specific location has yet been selected. Geological repositories are considered the safest method of long-term storage, as they isolate radioactive materials from the environment for thousands of years.

In the past, Bulgaria sent spent fuel to Russia for reprocessing. This process extracts valuable materials such as uranium and plutonium that can be reused. The remaining high-level waste is vitrified and returned for long-term storage.

Example from other countries:

Finland and Sweden are among the few countries that are already building geological repositories for high-level waste. These facilities are designed to ensure safety for tens of thousands of years.

Challenges and next steps

Public acceptance: The construction of long-term repositories often meets with resistance from local populations, which requires transparency and dialogue with society.

Geopolitical factors: Changes in international relations can affect the possibilities for exporting spent fuel for reprocessing [19].

Scientific research: The improvement of technologies such as transmutation can offer new solutions for reducing the radioactivity of waste.

Geological repositories are facilities designed for the long-term storage of high-level radioactive waste. They use natural geological formations that provide isolation of radioactive materials from the environment for thousands or even millions of years.

Geological repositories are built in stable rock formations, such as granites, clay marls or salt beds. These materials are resistant to erosion, earthquakes and water intrusion.

- Multi-level containment:
- Radioactive waste is encapsulated in durable containers made of materials such as steel or copper.
- The containers are placed in tunnels or shafts that are filled with barriers of concrete, bentonite clay or other insulating materials.
- Depth of storage:
- Repositories are usually located at a depth of 300 to 1000 meters below the earth's surface, which provides additional protection.
- Monitoring and control:
- Although repositories are designed for passive safety, they are actively monitored in the initial stages to ensure that no radioactive materials are released.

Latest technologies in radioactive waste management

1. Borehole disposal: This technology uses deep boreholes (up to 5 km) to store waste. This allows for deeper and more effective isolation compared to traditional geological repositories2.

2. Transmutation: An advanced method in which radioactive isotopes are converted into less radioactive ones through nuclear reactions. This significantly reduces the long-term hazard of the waste.

3. Vitrification: Radioactive waste is mixed with a glass material and heated to a high temperature to create a stable glass form that is resistant to leakage.

4. Robotic systems: Robots are used to handle and store waste in hazardous areas, minimizing the risk to humans.

5. Digital monitoring: Using sensors and artificial intelligence to continuously monitor the condition of the repositories and provide early warning of potential problems.

These technologies and approaches are aimed at ensuring maximum safety and sustainability in the management of radioactive waste [4], [20].

In Bulgaria and the Balkan Peninsula, various technologies are used for the management of radioactive waste, which meet international safety standards. Here is what is known:

In Bulgaria

1. Dry storage:

o In Bulgaria, spent nuclear fuel from the Kozloduy NPP is stored in special containers of the CONSTOR 440 type, which are resistant to corrosion and mechanical damage. This is the main method of temporary storage.

2. Reprocessing abroad: o In the past, Bulgaria sent spent fuel to Russia for reprocessing, but now long-term solutions are being sought in the country.

3. National repository for radioactive waste: o In Novi Han, there is a specialized repository for low- and intermediate-level waste, which meets modern safety requirements [6], [21].

In other countries on the Balkan Peninsula

1. Romania: Romania uses geological repositories for low- and intermediate-level waste. High-level waste is temporarily stored in dry repositories.

2. Serbia: In Serbia, temporary facilities are used for the storage of radioactive waste, including waste from medical and industrial sources.

3. Greece: Greece mainly manages low-level waste from medical and scientific sources, using temporary repositories.

4. North Macedonia: North Macedonia has small facilities for storing radioactive waste, mainly from medical applications.

Emerging technologies

- There are no geological repositories for high-level waste in the Balkans yet, but opportunities for regional cooperation are being discussed.
- Advanced technologies such as transmutation and vitrification are not widely implemented, but are seen as potential solutions for the future.

There are several significant projects related to the processing and storage of nuclear waste in the Balkan Peninsula and globally. Here are some examples:

Balkan Peninsula Projects

1. Bulgaria:

- National Radioactive Waste Repository: A modular repository for low- and intermediate-level waste is being built in the area of the Kozloduy NPP. This facility is designed to meet international standards and will be key to waste management in the country.
- Geological Repository: Bulgaria is considering the possibility of building a deep geological repository in areas such as Dobrudja or Strandzha. This is part of the long-term strategy for the management of high-level waste.

2. Romania: Romania has facilities for the temporary storage of high-level waste and is actively working on long-term management projects, including geological repositories.

3. Serbia and Greece: These countries mainly manage low-level waste from medical and scientific sources using temporary repositories.

Leading Countries in the World

1. Finland: Onkalo Project: This is the world's first deep geological repository for high-level waste, located in Olkiluoto. The project is an example of sustainable and safe management of radioactive waste.

2. Sweden: Sweden is developing a similar geological repository in the Forsmark area, which will store waste for tens of thousands of years.

3. France: CIGEO Project: France is building a deep geological repository in the Bür area, which will be one of the largest in the world.

4. USA: WIPP (Waste Isolation Pilot Plant): This is an underground repository in New Mexico that stores transuranic waste from military programs.

5. Japan: Japan is actively investing in vitrification and transmutation technologies to reduce the long-term radioactivity of the waste.

These projects demonstrate different approaches to nuclear waste management, focusing on safety and sustainability.

Reports and statistics on the quantities of radioactive waste generated worldwide are not centralized in a single universal table – the data are classified by type of waste (high-level, intermediate-level, low-level) and measured in different units (e.g., spent nuclear fuel in "metric tons of heavy metal" [MTHM], and low-level waste in cubic meters). The data are collected from multiple sources such as the International Atomic Energy Agency (IAEA), the Nuclear Energy Agency (NEA), and national radioactive waste management organizations. However, a rough overview of some of the estimates can be given, which will vary with time and collection methodology. The values below are approximate and serve only to illustrate the comparative scale of waste generated in major countries.

TABLE 1 APPROXIMATE QUANTITIES OF NUCLEAR WASTE

Country Spent nuclear fuel (MTHM)* Other radioactive waste (cubic meters)*	***Country Spent nuclear fuel (MTHM)* Other radioactive waste (cubic meters)****	***Country Spent nuclear fuel (MTHM)* Other radioactive waste (cubic meters)****
USA	~90,000	~250,000
France	~39,000	~90,000
Russia	~30,000	~120,000
Japan	~20,000	~60,000
United Kingdom	~15,000	~50,000
Germany	~10,000	~40,000
Total (world)	200,000+	700,000+

\It is important to note that:*

- "Spent nuclear fuel" is measured in MTHM (metric tons of heavy metal) – this represents the amount of nuclear material used in the fuel that has gone through the reactor cycle.
- "Other radioactive waste" includes waste from medical, industrial and research activities, as well as low- and intermediate-level nuclear waste; the measurement in cubic meters reflects the volume of their storage.

Comments and perspectives

1. Continuous updating of data: As new reactors enter or leave service, and decommissioning and spent fuel reprocessing continue, the values are updated periodically. IAEA and NEA central reports provide the most current information, but there is some variation in each publication depending on the methodology.

2. Different waste categories: Data for high-level waste (such as spent nuclear fuel) and low/intermediate-level waste are presented differently because the way in which it is generated, processed and stored differs by category and country.

3. Possibility of regional tables: Some countries or regional groups (e.g. the European Union) publish their own tables and reports, which can be found on their websites or in international publications. They focus not only on the quantity, but also on recycling, reprocessing and long-term storage strategies.

4. Recommended sources: For the most accurate and up-to-date information, it is recommended to consult the latest reports of the IAEA and NEA, as well as the national atomic energy agencies in individual countries.

In conclusion, although there is no universal and static table of radioactive waste generated for all countries, there are many assessment tables that are updated periodically. The sample table presented above provides an indicative comparison of the scale in some of the largest users of nuclear energy.

Nuclear waste recycling takes place in specialized facilities that are equipped to process spent nuclear fuel. Here are some key locations and prospects:

Where recycling takes place

1. France: France is a leader in nuclear waste recycling through facilities like those in The Hague. They extract valuable materials like uranium and plutonium that can be reused.

2. Russia: Russia has modern nuclear fuel reprocessing facilities that serve both domestic and international customers.

3. Japan: Japan is actively investing in recycling technologies, including vitrification of high-level waste.

4. USA: Although recycling is not widespread, the USA has pilot projects for nuclear fuel reprocessing.

Prospects for recycling

1. Technological innovation: Improvements in technologies like transmutation and vitrification could make recycling more efficient and safer.

2. Sustainable development: Recycling reduces the amount of high-level waste and supports nuclear energy as a low-carbon source.

3. International cooperation: Countries like Bulgaria can benefit from the experience of leading countries through partnerships and technology exchange.

4. Economic benefits: Recycling can reduce the costs of long-term storage and provide valuable resources for reuse.

IV. CONCLUSIONS

The conclusions on radioactive waste storage in Bulgaria and around the world can be summarized in the following areas:

1. The need for long-term solutions, because radioactive waste, especially high-level waste, requires safe management for thousands of years. Geological repositories are the most reliable long-term solution and are accepted as the standard in many countries.

2. Technological modernization, where dry storage and vitrification are proven methods for reducing the risk of leakage. Advanced technologies such as transmutation can significantly reduce the radioactivity of waste.

3. International cooperation, where countries like Bulgaria rely on imported technologies and knowledge exchange with countries like Finland, France and Sweden, which are leading in the construction of modern repositories.

4. Overcoming the challenges of public discussion and acceptance of the construction of radioactive repositories for intermediate and high-level radioactive waste, as the population of the selected region often opposes the construction of repositories. Transparency of proposals and discussions and public consultations are key to the successful implementation of these projects.The prospects for the industry can be summarized as:

1. Investment in innovation, where the development of technologies such as transmutation, borehole disposal and digital monitoring opens up new opportunities for safe management.

2. Sustainable development, because the recycling of spent fuel and the use of nuclear energy as a low-carbon source support the global transition to sustainable energy.

3. Expansion of geological repositories, because more countries are expected to build their own repositories for long-term storage, which will reduce dependence on waste exports.

4. Increasing public trust. By improving transparency, communication, and safety, the industry can strengthen citizens' confidence in nuclear energy.

Overall, the future of radioactive waste management will depend on a balance between innovation, effective planning, and social support.

ACKNOWLEDGMENTS:

This report is supported by the National Scientific Program "Security and Defense", approved by Decision No. 171/21.10.2021 of the Council of Ministers of the Republic of Bulgaria.

REFERENCES

[1] Annual Report NRA,the Council of Ministers, Sofia, 2015.

[2] Commission Regulation (Euratom) No 302/2005 of 8 February 2005 on the application of Euratom safeguards - Council/Commission statement, OJ L 054 28.02.2005 pp. 1-3.

[3] Commission Regulation (EC) No 1609/2000 of 24 July 2000 establishing a list of products excluded from the application of Council Regulation (EEC) No 737/90 on the conditions governing imports of agricultural products originating in third countries following the accident at the Chernobyl nuclear power station, OJ L 185 25.07.2000 pp. 27-39.

[4] Communication from the commission to the council and the european parliament. Communication on nuclear non-proliferation, Brussels, 26.3.2009, pp= 3-6.

[5] N. Dolchinkov, Investigation of the State of the Radiation Control Systems and the Actions of the Competent Authorities and the Population in the Event of a Change in the Radiation Background in Bulgaria, International conference Knowledge-Based Organization Subuy, Romania 24(3): pp.38-44

[6] N. Dolchinkov, N. Nichev, Gamma-background radiation control systems as a factor of Bulgaria's national security, Environment. Technology. Resources. Rezekne, Latvia, Proceedings of the 15th International Scientific and Practical Conference. Volume IV, Print ISSN 1691-5402, Online ISSN 2256-070X, pp. 83-88, DOI 10.17770/etr2024vol4.8225

[7] N. Dolchinkov, N. Nichev, Structure and Management of the National Automated System for Permanent Control of the Radiation Gamma Background in Bulgaria, De gruyter open, Land Forces Academy Review Vol. XXII, No 2(86), 2017, Sibiu, Romania, pp. 115-121.

[8] R. Marinov, S. Stoykov, P. Marinov, Urbanized territories non-existing part of crisis response operations, International Conference on Creative Business for Smart and Sustainable Growth, CreBUS 2019, 2019, 8840084

[9] N. Dolchinkov, Historical overview and analysis of national automated system for continuous monitoring of gamma radiation, VIII науково-практичного семінару з міжнародною участю "Економічна безпека держави і науково-технологічні аспекти її забезпечення“, Київ, 21-22 жовтня 2016 року ISBN 978-966-7166-38-0 pp. 220.228

[10] L. Lazarov, General Terms and Conditions for the Radio Connection Jamming, International Conference on High Technology for Sustainable Development, HiTech 2018 - Proceedings, 2018, 8566645

[11] D. Stefanova, V. Vasilev, I. Efremovski, Re-Innovative Organizational Design: Sustainable Branding and Effective Communication - Applied Models in a World With New Borders/Without Borders;; Book Chapter: Handbook of Research on Achieving Sustainable Development Goals With Sustainable Marketing, 2023, pp. 112–127; DOI: 10.4018/978-1-6684-8681-8.ch006;

[12] N. Todorov Dolchinkov, State of the population disclosure systems in the changing radiation situation in Bulgaria, Vide. Tehnologija. Resursi - Environment, Technology, Resources, 2019, 1, pp. 54–58

[13] N. Dolchinkov, Modernization of monitoring and public notification systems in case of radioactive pollution of the environment in Bulgaria, Scientific and Practical Journal “Global Nuclear Safety”, No. 3 (24) 2017, Moscow, MEPI, Russia, pp 7-18.

[14] S. Stoykov, The System Of Education, Training And Research In The Field Of Security - Managing Change Through Experience And Knowledge, Vide. Tehnologija. Resursi - Environment, Technology, Resources, 2024, Volume 4, pp. 269–274, Print ISSN 1691-5402, Online ISSN 2256-070X, DOI: https://doi.org/10.17770/etr2024vol4.8213

[15] N. Dolchinkov, Optimization of the systems for monitoring and public disclosure of radioactive contamination of the environment,International journal „Knowledge “, Skopie ISSN 1857-92 Vol 15.1 p. 423-431 GIF 1.023 (2015) . Available: https://www.researchgate.net/publication/320378173

[16] S. Vambol, N. Dolchinkov, V. Vambol, S. Abbas, S. Yeremenko, O. Trush, Mathematical modeling study of the process of transfer radioactive contamination from the Chernobyl accident zone, Journal of Mountain Area Research, ISSN: 2518-850X (Online), 2518-8496 (Print), 2024

[17] N. Dolchinkov, Optimizing energy efficiency in the conditions of a global energy crisis, Optimizing Energy Efficiency During a Global Energy Crisis, 2023, ISBN13: 9798369304006 EISBN13: 9798369304013, DOI: 10.4018/979-8-3693-0400-6 pp. 1–9.

[18] N. Padarev, Anthropogenic accidents and catastrophes, PIK Publishing House, VT, 2016, pp 5- 235.

[19] M. Pavlov, The radiation consequences of accidents at nuclear power plants and the use of nuclear weapons, Scientific conference "Radiation safety in the modern world", NSU "V. Levski" - city of V. Tarnovo - November 22, 2019 ISBN 2603-4689, pp. 84-90

[20] S. Lilianova, N. Padarev, Radiation incidents with radioactive waste Collection of reports from a scientific conference of the National University "V. Levski", Volume 4, V. T. 2018, ISBN 1314-1937

[21] V. Vasilev, D. Stefanova, M. Icheva, Green human resource management as a component of sustainable organizational development in environmental and natural economics, ETR, vol. 1, Jun. 2024, pp. 402–407 DOI: 10.17770/etr2024 vol1.7966

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025 Volume V, 89-96

Using Drones to Clean Continental Water Bodies

Nikolay Todorov Dolchinkov
Vasil Levski National Military University, Veliko Tarnovo, Bulgaria
Veliko Tarnovo, Bulgaria
n_dolchinkov@abv.bg

Nikolay Bonev Nichev
"Georgi Benkovski"
Bulgarian Air Force Academy: Bulgaria
Dolna Mitropolia, Bulgaria
nicheff@abv.bg

***Abstract*— Pollution of continental water bodies has become increasingly widespread in recent decades. Plastic, construction, household and other waste is being dumped uncontrollably both near water bodies and directly into them. In addition to pollution, this often leads to more serious crisis and emergency situations such as floods, pollution of drinking and groundwater, landslides and others. This article proposes a new application of mid-range drones for monitoring pollution, the presence of unregulated landfills and transmitting information in real time. In this way, it will be possible to monitor large areas for the presence of illegally dumped waste with fewer resources. This will help to more effectively combat unregulated landfills and solve the problem in its infancy and save financial and human resources.**

Keywords*— *continental water bodies, drone, groundwater, landfill, pollution, waste, water resources.

I. INTRODUCTION

In recent decades, unmanned aerial vehicles have been increasingly widely used. They are relatively light, maneuverable, and their price is becoming lower and more affordable. These modern technical means are being used in more and more areas, including the military industry [1], [2]. This is also proven in the military operations that are taking place in Ukraine, the Gaza Strip, and other hot spots on our planet. But at the same time, various modifications of unmanned aerial vehicles are also required in the civilian sector of the economy, as well as in the field of services, cartography, and other areas of our lives [3], [4]. Drones, as a type of unmanned aerial vehicle, have many modern applications that significantly facilitate various aspects of our lives and work.

First of all, the use of drones in the delivery of goods can be put, for example, the companies Amazon and UPS use them for fast and efficient delivery of goods to customers. In this way, they significantly reduce delivery time.

It can be said that the use of drones in agriculture is also increasing significantly. There, drones help farmers monitor and analyse crop conditions, as well as spray fertilizers and pesticides. They are replacing the use of agricultural aviation for fertilization, but smaller farmers still use ground transportation equipment more often. But for larger farmers, the use of unmanned aerial vehicles is becoming a cheaper option and also more efficient [5], [6].

In recent years, there has been an increasing emphasis on environmental monitoring. Here, they are used to monitor natural resources, forest fires and pollution in areas that are difficult to access with conventional equipment, while at the same time providing a better view of the monitored component. This is also the purpose of this work, which shows the possibilities of using these aircraft to detect unregulated dumps in water bodies or in their immediate vicinity. With conventional means, detecting these pollutants is sometimes difficult, and their consequences can be very serious [7], [8]. This is especially true for non-degradable and plastic waste.

Drones can be used to search and rescue people in hard-to-reach areas, in the event of natural disasters, such as avalanches, earthquakes, floods and others. This method is especially valuable for mountain rescuers during the winter season.

Next, infrastructure inspections can be mentioned. They are used to inspect bridges, buildings and other infrastructure sites, which saves time and resources. This is especially important for hard-to-reach sites where it is not possible to examine certain nodes and details in detail [9], [10].

Filming and photography: Drones are popular in the film industry and photography for capturing unique aerial shots and are increasingly used to film films, series and short advertising videos.

Yes, drones can be used to monitor environmental pollution. They can be equipped with specialized sensors

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8501
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

and cameras that can measure various pollution parameters, such as air, water and soil quality, the content of certain ingredients in them and others. When monitoring air, drones and in particular the equipment they carry can measure the concentration of pollutants such as carbon dioxide, nitrogen oxides and dust particles. When monitoring water, they can collect samples from water bodies and measure parameters such as pH, temperature, the presence of toxic, hazardous or other substances, the presence of amounts of non-degradable waste and others. When conducting soil monitoring, drones can analyse the condition of the soil and detect contamination with heavy metals and other harmful substances, using equipment located on them or transporting samples from the field.

Their use is particularly relevant in radiation monitoring [11], [12]. After natural disasters with the release of radioactive substances, drones can be used to detect and map radiation hotspots by surveying large areas and transmitting information in real time [13].

The use of unmanned aerial vehicles and equipment located on them allows for fast and efficient data collection, which helps to better manage and protect the environment. Thus, personnel do not enter the contaminated area, are not exposed to radioactive radiation, and very good results are obtained from the measuring equipment without danger to the population.

It should be noted that there are also successful projects that demonstrate the effectiveness of drones in environmental monitoring:

1. The ICAERUS project is funded under the Horizon Europe program, this project supports innovative solutions with drones in agriculture and forestry. It involves partners from 8 countries and aims to explore the possibilities of using drones for environmental monitoring.

2. The SPADE project, also funded under Horizon Europe, this project promotes the use of drones and sustainable digital services in the crop, forestry and livestock sectors. The project brings together 21 partners from 10 countries.

These projects show how drones can be used for effective environmental monitoring and management.

Drones are also used in Bulgaria to monitor environmental pollution, albeit on a limited scale. For example, the Sofia Metropolitan Inspectorate uses drones to monitor air quality and to detect illegal waste burning. These drones are equipped with sensors and cameras that can detect pollutants and locate sources of pollution [14], [15].

II. MATERIALS AND METHODS

The use of this type of equipment is expanding extremely quickly and several leading companies can be mentioned that offer environmental monitoring services with drones. A long list could be made here, but we should first mention ZaiTechno, which offers radiation monitoring drones that can detect and map radiation hotspots and pollution. The company Copter.bg offers various drones and solutions for environmental monitoring, including aerial photography and mapping. There are other successful companies, but I believe that they will still expand and cover an increasingly larger perimeter of services.

Various methods and technologies can be used to monitor environmental pollution with drones. Here are some of them:

1. Drones can be equipped with air quality sensors that measure the concentration of pollutants such as carbon dioxide, nitrogen oxides and particulate matter. These sensors provide real-time data on air quality.

2. Thermal cameras can detect thermal anomalies that may be associated with pollution, such as chemical leaks or hot spots in industrial areas, chemical reactions taking place in unregulated conditions, and the release of large amounts of heat.

3. Multispectral and hyperspectral cameras can capture images in different spectral ranges, which allows for the detection of water and soil pollution, as well as vegetation analysis.

4. Water sensors can be deployed in drones and collect samples from water bodies and measure parameters such as pH, temperature and the presence of toxic substances. This is particularly useful for monitoring pollution in rivers, lakes, seas and other bodies of water.

5. After natural disasters or near nuclear facilities, drones can be equipped with radiation detectors to detect and map radiation hotspots. This is also a good way to periodically monitor the radiation situation.

6. Lidar technology uses laser beams to create three-dimensional maps of the terrain and can be used to detect changes in the landscape that may be associated with pollution.

This is just some of the methods used, and this allows for fast and efficient data collection, which helps to better manage and protect the environment. It is also possible to collect other types of data, which may be regional in nature, or to develop new detectors to study other environmental parameters [2], [15], [16].

One of these parameters is environmental pollution with non-degradable plastic, nylon and other waste in water bodies or in the catchment areas of drinking areas. This problem is of great importance for Bulgaria in connection with climate change, reduction of water resources and their inefficient use. Different types of drones and methods can be used to detect waste dumps near water bodies. Here are some of the most important ones, because it is impossible to list them all, and each case requires a specific solution [3], [17].

In this area of application of drones, the following can most often be used:

• Multicopters are maneuverable and can fly at low altitudes, which makes them suitable for detailed terrain photography and detection of waste dumps. They are

especially suitable for forested areas, mountain stream beds and overgrown and difficult-to-reach banks of water bodies.

• Fixed-wing drones can cover larger areas and are suitable for monitoring large areas around water bodies and above the water bodies themselves.

• Hybrid drones combine the advantages of multicopters and fixed-wing drones, which makes them effective for various tasks and they have the widest application.

There are different detection methods, the most common of which are:

• In visual photography, drones can be equipped with high-quality cameras that capture images and videos of the terrain. This data can be collected and analysed, thus monitoring the development of the area and serving for timely changes in the situation and detection of waste dumps.

• Thermal cameras can detect temperature anomalies that may be associated with waste dumps, especially if there is waste incineration. With the help of these cameras, the conception of fires can be detected and good preventive action can be taken to prevent large outbreaks of fires.

• Multispectral and hyperspectral cameras can capture images in different spectral ranges, which allows the detection of pollution and waste dumps.

• Lidar technology uses laser beams to create three-dimensional maps of the terrain and is very well used to detect changes in the surrounding environment and especially the formation of new waste dumps.

Although in its infancy, these technologies have already found application in the implementation and management of several successful projects. In the municipality of Yambol, drones are used to monitor illegal waste disposal and the formation of landfills. These drones are equipped with cameras and other sensors that allow for effective monitoring [7], [18]. So far, there are no known cases of successful implementation of similar projects in other municipalities, but the first successful applications will give impetus to the use of these new methods for detecting illegal landfills around water bodies [19].

These technologies and methods allow for the quick and effective detection of waste dumps, which helps to better manage and protect the environment. In this way, with regular monitoring, such illegal landfills can be detected at an early stage and their expansion prevented.

After researching different types of unmanned aerial vehicles, their characteristics and the task at hand, several specific drones are proposed as the best options. For detecting waste dumps in or near water bodies, some of the most suitable drones are:

1. DJI Matrice 300 RTK is a drone that is known for its stability and ability to carry various sensors and cameras, including thermal and multispectral cameras.

2. SenseFly eBee X is a drone that has fixed wings and is suitable for covering large areas and can be equipped with various sensors for environmental monitoring.

3. Parrot Anafi USA is a drone that is equipped with thermal and optical cameras, making it suitable for detecting waste dumps and monitoring pollution.

The methods for detecting contaminated areas in water bodies and adjacent areas are diverse and sometimes even specific to the specific case [20]. But they can be systematized into several main categories:

1. Visual imaging uses high-quality cameras to capture images and videos of the terrain, which can be analysed to detect waste dumps. The image can be stored on a carrier that is located on the drone or the information can be transmitted using electromagnetic waves with a certain frequency.

2. Thermal imaging cameras are used to detect temperature anomalies associated with waste dumps, especially if there is waste incineration and heat energy is released.

3. Multispectral and hyperspectral cameras are used to capture images in different spectral ranges to detect pollution and waste dumps.

4. Lidar technology is used to create three-dimensional maps of the terrain where non-degradable waste may be located.

These drones and methods allow for efficient and rapid detection of waste dumps, which helps to better manage and protect the environment. Regular site surveys can detect the creation of such landfills at an early stage and timely preventive measures can be taken. This way, the disposal of plastic, nylon and other hard-to-degrade waste can be significantly limited.

III. Results and discussion

Detecting unregulated dumping sites for persistent substances is a difficult, and sometimes almost impossible, way to limit environmental pollution. The use of unmanned aerial vehicles greatly facilitates this task. To make drones more effective for environmental monitoring, various sensors and components can be added, the most commonly used sensors being:

1. Air quality sensors measure the concentration of pollutants such as carbon dioxide, nitrogen oxides, particulate matter, and other components of the ambient air.

2. Water sensors can collect samples from water bodies and measure parameters such as pH, temperature, and the presence of toxic, poisonous, or other substances.

3. Radiation detectors detect and map radiation hot spots, which is useful after natural disasters or near nuclear facilities.

4. Thermal cameras use infrared sensors to detect thermal anomalies, which is useful for detecting waste dumps and pollution.

5. Multispectral and hyperspectral cameras capture images in different spectral ranges, which allows for analysis of vegetation, water and soil.

In addition to sensors for obtaining reliable, real and timely information, other components are also used to supplement, process, transmit or enrich the information received. As such, GPS modules are very often used, which serve for accurate positioning and navigation of both the drone itself and the monitored objects. Another example is the use of the LIDAR system, which is used to obtain high-quality images of the environment in all projections and monitor the state of nature in and around water bodies. Various communication systems and channels are used to transmit data in real time to ground stations or mobile devices. In this way, the collected information is transmitted to the control centre, where it is summarized and analysed. This is achieved by using appropriate data analysis software. It serves to process and visualize the collected data, which facilitates analysis and decision-making [21].

The use of various sensors and components makes drones more efficient and versatile for various environmental monitoring tasks. In this way, we can obtain a large volume of quality information with specific data and the development of this data over time in a short time [22].

Thermal cameras are one of the most commonly used components for environmental monitoring and they work on the principle of capturing infrared radiation emitted by objects depending on their temperature. They convert this radiation into electrical signals that are used to create a visual image called a thermogram. The principle by which thermal cameras detect water bodies contaminated with plastic waste can be explained in several ways, each of which is correct and complements the others. The first explanation is the presence of temperature differences. Plastic waste and water have different temperature characteristics. Thermal cameras can detect these differences and visualize them as thermal images. Plastic waste usually appears as colder or warmer objects compared to water during different seasons of the year and is not at the same temperature as water.

Thermal cameras can also detect thermal anomalies that may be associated with the presence of plastic waste. For example, large accumulations of plastic can change the thermal profile of a body of water, and hence this temperature difference can manifest.

Thermal cameras create infrared images that show the temperature differences between the water and the plastic waste. These images can be analysed to detect pollution. Experienced analysts can easily detect the presence of plastic waste in bodies of water from thermal camera images alone.

The most common use is in monitoring bodies of water and examples of use such as monitoring rivers and lakes. Thermal cameras can be used for regular monitoring of bodies of water to detect and map plastic waste.

Another example is in detecting pollution in marine areas. They can be used to detect plastic waste in coastal and marine areas, where pollution is more difficult to monitor with traditional methods.

These technologies allow for rapid and effective detection of pollution with regular monitoring, which helps to better manage and protect the environment.

Other types of cameras for detecting plastic waste in water bodies are:

1. Multispectral cameras capture images in different spectral ranges, allowing the detection of plastic waste and other pollutants in water. They are particularly useful for analysing vegetation and water bodies.

2. Hyperspectral cameras provide more detailed spectral data than multispectral cameras and can detect specific types of plastics and other pollutants in water.

3. High-quality RGB cameras can capture detailed images of water bodies, which can then be analysed for the presence of plastic waste. They are useful for visual inspections and monitoring.

4. Satellites equipped with different types of cameras and sensors can provide data over large areas of water and detect accumulations of plastic waste in oceans and coastal areas. Artificial intelligence can help analyse these images and detect pollution.

These technologies and methods allow for effective and rapid detection of pollution, which helps to better manage and protect the environment. Collecting all the information on a carrier on the drone carries significant risks of information loss, and therefore continuous transmission of information from the drone to the control centre is preferred, and different types of communication networks can be used:

1. Radio communication is the most commonly used method of data transmission is via radio. Drones use different frequency ranges (for example, 2.4 GHz or 5.8 GHz) to communicate with the ground station.

2. Some drones use mobile networks such as 4G or 5G networks for real-time data transmission. This is particularly useful in urban environments or areas with good mobile coverage.

3. For drones operating in remote or difficult-to-reach areas, satellite communication is a reliable method of data transmission. However, this method is more expensive and requires specialized equipment.

4. In some cases, drones can use Wi-Fi networks for data transmission, especially when operating near infrastructure with an available Wi-Fi signal.

This type of aircraft has great advantages in detecting unregulated landfills and pollution of water bodies with plastic, nylon and other difficult-to-degrade waste. However, there are areas in these areas where the signal strength for controlling the drones is absent or very weak. This is especially important for rugged forested areas, mountainous areas or areas remote from settlements. When

operating in such hard-to-reach areas with reduced visibility or limited signal, other techniques are used to control the aircraft, transmit information from them and other details of the flight and transmit information [4], [23].

The most common are autonomous flights, in which drones can be programmed for autonomous flights along preset routes. This reduces the dependence on constant connection with the operator and makes it possible to complete the task even in the absence of any type of connection.

Using RTK (Real-Time Kinematic) GPS is the next most commonly used method. This technology provides high positioning accuracy and is useful in areas with limited signal, such as mountainous areas and rugged terrain. In areas with limited signal, where regular flights and data collection are carried out, repeaters can be used to amplify and transmit the signal between the drone and the ground station or operator. These repeaters can be stationary or mobile depending on the frequency of flights, terrain and other factors affecting the flight.

Thermal and infrared cameras are another type of alternative to classical methods, which are also used in collecting information about the pollution of water bodies. In conditions of reduced visibility, thermal and infrared cameras can help navigate the aircraft and detect objects in low visibility.

For real-time data transmission from remote and hard-to-reach areas, satellite communication is a reliable method, although it is more expensive. As technology advances, this method is used more and more often and its price has decreased over the years. One of the main advantages of this method is that it can be used practically almost anywhere on the planet and the quality of the transmitted information is at a high level.

These methods and technologies allow for effective operation of drones even in hard-to-reach areas and under adverse conditions. This is one of the reasons for the increasing use of unmanned aerial vehicles in various areas of our lives, including for monitoring environmental pollution with non-degradable waste. In practice, the use of drones in military operations in Ukraine proves the capabilities of drones in all areas, including military affairs.

Ensuring the safety of drone flights is essential. With the use of more and more drones, the thesis of their safe use is also required, including legal regulation of these flights. With the development of aircraft, systems for safe flying with them and with other participants in aviation are also developing [24].

With the increase in the number of drones and the flights they perform, collision avoidance systems are also improving. Many drones are equipped with obstacle avoidance sensors that use ultrasound, infrared rays or lidar to detect and avoid obstacles during flight. In this way, they change the trajectory of their flight and avoid collisions with obstacles or other aircraft.

With the increasingly widespread use of drones, geofencing is also required. This is a technology that restricts drone flights in certain areas, such as airports, military bases and other sensitive sites. Geofencing helps prevent incidents and airspace violations, such as the one that occurred at Sofia Airport 2 months ago, when a drone violated the airspace of the airport complex and disrupted air traffic for hours.

Many drones have an automatic return-to-home function that is activated when the signal is lost or the battery is low. This ensures that the drone will return safely to the take-off point without the need for navigation. This is an autonomous function that limits the possibility of losing the drone in the airspace over a certain territory.

Training and certification also play an exceptional role in the normal operation of these aircraft. Drone pilots must undergo training and obtain certificates for drone control, especially for professional and commercial flights. People who operate drones for monitoring must be well trained and have a certificate to operate the specific type of aircraft.

Working in adverse weather conditions is also key. To monitor pollution of water bodies and adjacent areas, favourable weather conditions should be used whenever possible. In adverse weather conditions, flights should only be carried out in extreme cases and, if possible, they should be cancelled for more favourable conditions [25].

Choosing the right drone is especially important when working in adverse conditions. For operations in adverse weather conditions, it is important to choose a drone that is resistant to wind and rain. Larger and more stable drones are better suited to such conditions. It is also a good idea for the aircraft to have additional flight control systems.

Thermal and infrared cameras can be very helpful for navigation and detection of objects in reduced visibility, such as fog or darkness. For each flight, the cameras should be selected according to the type of activity the drone will perform and the weather conditions of the flight.

For real-time data transmission in low visibility and bad weather conditions, satellite communication is a reliable method, although it is more expensive.

Drones can be programmed to fly autonomously along preset routes, which reduces the dependence on constant communication with the operator and is not affected by weather conditions [26], [27].

These measures and technologies help ensure flight safety and the effective operation of drones even in adverse weather conditions. However, legal regulation of the use of drones is also necessary, because at some point chaos will occur in the airspace and then regulation will be more difficult [28], [29], [30].

Based on a study, the most suitable drones for monitoring pollution of water bodies and adjacent areas in bad weather can be indicated:

1. DJI Matrice 300 RTK is a drone known for its stability and resistance to wind and rain. It is equipped with

multiple sensors for avoiding obstacles and can operate in severe weather conditions.

2. DJI Mavic 2 Enterprise Dual is a drone equipped with a thermal camera and is resistant to wind and rain. It is suitable for rescue operations and monitoring in bad weather conditions.

3. Parrot Anafi USA is also a drone resistant to wind and rain and is equipped with thermal and optical cameras, which makes it suitable for operation in harsh conditions3

When flying in bad weather conditions such as fog, heavy rain or snowfall, safe flight conditions must also be observed above all and flights should not be carried out if possible. For example, flying in fog is difficult due to reduced visibility and drones with thermal and infrared cameras can help navigate in such conditions. Many drones are not waterproof and can be damaged by heavy rain. For flying in the rain, it is important to use drones that are specially designed for such conditions. The requirements for flying in snow are similar, because it can be dangerous due to reduced visibility and the risk of freezing of drone components. Drones with cold-resistant components and thermal cameras can help operate in such conditions.

In the process of conducting the study, it was found that in Bulgaria, in addition to the municipality of Yambol, the Sofia municipality and the Municipality of Burgas use marine drones and artificial intelligence to detect potential risks of pollution of habitats in the Black Sea. This initiative is part of a project in support of the blue transformation of the Black Sea basin. These are still the first tests for the use of drones in this area, but it always starts small.

In Europe, the Copernicus Marine Service is one of the monitoring systems that uses unmanned aerial vehicles. In the countries of the old continent, various techniques are used for monitoring plastic waste, including numerical modeling, on-site monitoring and satellite monitoring. These methods help to track the movement of plastic waste and assess its quantity. The prospect is to monitor more and more water bodies and the space around them for the presence of non-degradable waste, and a significant part of the monitoring will be carried out with drones.

Different technologies are used around the world to detect plastic waste in the oceans. For example, ocean current modelling and satellite observation are key methods for tracking plastic waste and assessing its impact on marine ecosystems. Using satellite images, islands of plastic waste in the oceans and seas can be easily detected. In coastal areas, especially in the Pacific region with lush tropical vegetation, the use of drones for monitoring the coastal zone is of utmost importance and is increasingly being used [31], [32].

Some of the more significant successful examples and projects include:

The LIFE-funded HESOFF project uses drones to remotely image forests and assess their health. This project shows how drones can help conserve biodiversity and manage forest resources.

WWF projects use drones to monitor forests and wildlife in different parts of the world. These projects demonstrate how drones can be effective tools for environmental protection and combating climate change.

These technologies and methods allow for effective detection and monitoring of plastic waste pollution, which helps to better manage and protect the environment.

IV. CONCLUSIONS

The future of drones in environmental protection looks promising, as they are expected to play an increasingly important role in various aspects of environmental monitoring and management. Based on the study conducted, the analysis of the results achieved so far in the use of drones for detecting plastic waste, and the assessment of the future use of these progressive technologies, some conclusions and recommendations can be drawn for the development of the use of these techniques and technologies. Here are some key trends and technologies that will shape the future of drones in this area based on this study:

1. With the development of artificial intelligence and machine learning, drones will become increasingly autonomous, which will allow them to perform complex tasks without the need for constant human control. It will be necessary for a person to set the parameters of the task and control its execution, and the activities themselves will be performed by autonomous drones

2. Drones will be connected and integrated with IoT (Internet of Things), with networks of sensors and other devices, which will allow for the collection and analysis of data in real time for better environmental management. This will allow for larger databases to be collected, which will make research more accurate and forecasts better.

3. The development of new and more sensitive sensors and cameras will allow for more precise detection and monitoring of pollution and other environmental problems. Less time and resources will be needed to assess the situation and make an adequate decision.

4. Drones will increasingly use renewable energy sources, such as stand-alone solar panels, to reduce their carbon footprint and be more environmentally friendly.

As prospects for the use of drones in the foreseeable future, the following can be mentioned:

1. Drones will continue to play a key role in the detection and monitoring of air, water and soil pollution. They will be an indispensable tool for detecting pollution of water bodies and their adjacent territory by plastic waste.

2. They will be used to track wildlife populations and detect illegal activities such as poaching. They will help to expand biodiversity and preserve the purity of the environment.

3. Drones will help to quickly assess damage after natural disasters and plan restoration activities. They will help to locate injured people and rescue them.

These trends and technologies show that drones will continue to be an important tool in efforts to protect the environment and sustainably manage natural resources.

In Bulgaria, work is underway to increase the use of drones in state, municipal and private structures, and they are also used in a number of projects, and emphasis will be placed on several of them:

A project for the blue transformation of the Black Sea basin has the Municipality of Burgas as the main beneficiary. Municipal administration employees are using marine drones and artificial intelligence to detect potential risks of pollution of habitats in the Black Sea. This project is part of a larger initiative to protect the marine environment and is about to be expanded.

The HESOFF project, which is funded under the LIFE program and monitors the environment, including water bodies. This project involves remote sensing of forests with unmanned aerial vehicles to assess the health of forests, the state of water bodies in them and the protection of biodiversity.

These projects show how Bulgaria strives for sustainable development and environmental protection through innovation and new technologies, including the use of unmanned aerial vehicles. Based on the research conducted, the analysis of the results obtained and the identified prospects for the use of drones in environmental monitoring, and in particular of water bodies and adjacent terrains, we can summarize that a wider use of drones in environmental protection is imminent.

ACKNOWLEDGMENTS:

This report is supported by the National Scientific Program "Security and Defense", approved by Decision No. 171/21.10.2021 of the Council of Ministers of the Republic of Bulgaria.

REFERENCES

[1] L. Poiša, A. Adamovičs, L. Antipova, G. Šiaudinis, D. Karčauskienė, R. Platače, A. Žukauskaitė, S. Malakauskaitė, Ē. Teirumnieka, The chemical content of different energy crops, Environment. Technology. Resources. Rezekne, Jun 2015, Latvia. Proceedings of the 8 th International Scientific and Practical Conference, vol 1, pp. 191-196, 2011. https://doi.org/10.17770/etr2011vol1.913

[2] E. Cubars, L. Poiša, Analysis of Composite Biomass Fuels Properties, Environment. Technology. Resources. Rezekne, Jun 2019, Latvia. Proceedings of the 12 th International Scientific and Practical Conference, vol. 1, pp. 39–43, Jun. 2019, doi: 10.17770/etr2019vol1.4043

[3] A. Adamovics and L. Poisa, Evaluation of chemical content in different energy crops. In: The 8th International scientific conference "Rural development 2017: Bioeconomy Challenges": abstracts book, Kaunas, Lithuania, 23-24th November, 2017 Aleksandras Stulginskis University, Ministry of Agriculture of the Republic of Lithuania, Kaunas,2017, pp. 199.-202.

[4] V. Vasilev, D. Stefanova, and M. Icheva,. Green human resource management as a component of sustainable organizational development in environmental and natural economics, ETR, vol. 1, pp. 402–407, Jun. 2024, doi: 10.17770/etr2024vol1.7966

[5] S. Stefanova, V. Vasilev, I. Efremovski. Re-innovative organizational design: sustainable branding and effective communication - applied models in a world with new borders/without borders, Book Chapter: Handbook of Research on Achieving Sustainable Development Goals With Sustainable Marketing, 2023, pp. 112–127; DOI: 10.4018/978-1-6684-8681-8.ch006

[6] L. Poisa and A. Adamovics, Ash melting behaviour oxidizing atmosphere in energy crops . 11th International scientific conference "Engineering for rural development" : proceedings, Jelgava, Latvia, May 24 - 25, 2012 [elektroniskais resurss] / Latvia University of Agriculture. Faculty of Engineering. - Jelgava, 2012. - pp.506.-510.

[7] R. Platace, L. Poisa, A. Adamovics, Reed canary grass (Phalaris arundinacea L.) productivity and quality depending on agro-meteorological conditions, 11th International scientific conference "Engineering for rural development" : proceedings, Jelgava, Latvia, May 24 - 25, 2012, Latvia University of Agriculture. Faculty of Engineering, Jelgava, pp. 195-198, 2012.

[8] N. Dolchinkov, Construction Of A System For Monitoring The Pollution Of Water Bodies With Waste, Environment. Technology. Resources. Rezekne, Latvia, Proceedings of the 15th International Scientific and Practical Conference. Volume I, Print ISSN 1691-5402, Online ISSN 2256-070X, pp 136-141, https://doi.org/10.17770/etr2024vol1.7989

[9] N. Dolchinkov, Optimizing energy efficiency in the conditions of a global energy crisis, Optimizing Energy Efficiency During a Global Energy Crisis, 2023, ISBN13: 9798369304006 EISBN13: 9798369304013, pp. 1–9, DOI: 10.4018/979-8-3693-0400-6

[10] M. Popova, Australia collects plastic waste, Green World, No. 2, pg 13, 2020;

[11] N. Nikolov, Determining the toxicity class of industrial waste, Collection of reports from the Annual University Scientific Conference, volume 5, Publishing Complex of the Vasil Levski National University, 2020, pp. 177-181, ISSN 1314-1937;

[12] N. Dolchinkov, B. Karaivanova-Dolchinkova, Impact of Types of Electromagnetic Radiation on Living Nature, 14th International Scientific and Practical conference Environment. Technology. Resources. Vide. Technology. Resursi, 2023, ISSN 1691-5402, 1, pp. 55–59

[13] M. Haralampiev, Global environmental problems and their relationship with the protection of the population and infrastructure, Collection of reports from the scientific conference "Actual problems of the protection of the population and infrastructure", Vasil Levski, Veliko Tarnovo, 2012, volume 4 , pp. 34-49, ISBN 978-954-753-104-8;

[14] N. Dolchinkov, N. Ozerova, State of recycling of waste in Bulgaria, International scientific journal: Science. Business. Society 4/2019, ISSN 2367-8380 pp. 131-134;

[15] N. Padarev, Anthropogenic accidents and catastrophes, PIK Publishing House, VT, 2016, pp. 235.

[16] R. Marinov, S. Stoykov, P. Marinov, Urbanized territories non-existing part of crisis response operations, International Conference on Creative Business for Smart and Sustainable Growth, CreBUS 2019, 2019, 8840084

[17] N. Todorov, State of the population disclosure systems in the changing radiation situation in Bulgaria, Vide. Technology. Resources - Environment, Technology, Resources, 2019, 1, pp. 54–58

[18] S. Stoykov, Risk management as a strategic management element in the security system, International Conference on Creative Business for Smart and Sustainable Growth, CreBUS 2019, 2019, 8840098

[19] S. Stoykov, The System Of Education, Training And Research In The Field Of Security - Managing Change Through Experience And Knowledge, Vide. Tehnologija. Resursi - Environment, Technology, Resources, 2024, Volume 4, pp. 269–274, Print ISSN 1691-5402, Online ISSN 2256-070X, DOI: https://doi.org/10.17770/etr2024vol4.8213

[20] G. Vassilev, Radio ecology, Tita consult, Sofia, 2005;

[21] V. Vasilev, D. Stefanova, C. Popescu, Human capital management and digitalization - From good practices and traditions to sustainable development; Book Chapter: Digitalization, Sustainable Development, and Industry 5.0: An Organizational Model for Twin Transitions, 2023, pp. 41–65; https://doi.org/10.1108/978-1-83753-190-520231004

[22] B. Dimitrov, Problems in the special preparation for nuclear, chemical and biological protection, Collection of reports from a scientific conference, IV International Scientific Conference High Technologies. Business. Society 11-14.03.2019, Borovets, Bulgaria, Volume Iii "Society", pp. 263-265, ISSN 2535-0005

[23] O. Loktionov, E. Fedotova, O. Kondrateva, N. Dolchinkov, N. Kuznetsov. Actual and design wind loads for overhead transmission lines in the Central European part of Russia, IOP Conference Series: Earth and Environmental Science This link is disabled., 2023, 1281(1), 012050

[24] L. Poiša, L. Antypova, Evaluation of the Effects of Herbicides on the Weeds and the Productivity of Hybrids Maize. Environment. Technology. Resources. Rezekne, Latvia. Proceedings of the 14 th International Scientific and Practical Conference, vol. 1, pp. 195–199, Jun. 2023, doi: 10.17770/etr2023vol1.7204.

[25] G. Stanchev, Technical obstacles to speech intelligibility, Environment. Technology. Resources. Proceedings of the 15th International Scientific and Practical Conference June 27-28, 2024, Vol. 3, pp 300-305

[26] M. Simeonov, M. Marinov, Determine the location of nodes in wireless sensor network by using genetic algorithm, Environment. Technology. Resources. Proceedings of the 15th International Scientific and Practical Conference June 27-28, 2024, Vol. 2, doi.org/10.17770/etr2024vol2.8059 pp 247-252

[27] N. Nichev, K. Koynakov, Use of Unmanned Aircraft in the Logistics Support of Military Formations, Eurasia Proceedings of Science, Technology, Engineering and Mathematics, , 2024, 31, pp. 92–99

[28] B. Sawicka, M. Messaoudi, V. Vambol et all, Organic Micropollutants in Wastewaters: Advances in Sustainable Management and Treatment Methods, Organic Micro Pollutants in Aquatic and Terrestrial EnvironmentsPages 225 - 2471 January 2024

[29] N. Tonchev, N. Teirumnieks, E. Yankov, Modeling the Hardening of Carbon Steels After Quenching and Tempering, Vide. Tehnologija. Resursi - Environment, Technology, Resources, , 2024, 3, pp. 456–459

[30] N. Dolchinkov, M. Pavlov, Study of the Influence of Winds in the Potential Contamination with Hazardous Substances as A Result of Man-Made Accidents, Vide. Tehnologija. Resursi - Environment, Technology, Resources, , 2024, 1, pp. 130–135

[31] S. Madzharov, I. Ivanov, N. Yordanov, A Digitally Manipulated Gunshot Sound Identification. In ENVIRONMENT. TECHNOLOGIES. RESOURCES. Proceedings of the International Scientific and Practical Conference, 2024, Vol. 3, pp. 170-174 , ISSN: 16915402 , DOI: 10.17770/etr2024vol3.8150 .

[32] T. Trifonov, I. Simeonov, N. Yordanov, Advanced signal processing methods for analysis of high dynamic range acoustic phenomena , Communication, Electromagnetics and Medical Application, 2018, October, pp. 52–56.

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 97-101

Analysis of the Possibilities for Visualizing the Risk of Disasters and Accidents in the Areas of Critical Infrastructure Sites Through GIS Applications

Grigor Grigorov
Logictic and Technology Faculty
Vasil Levski National Military University
Veliko Tarnovo, Bulgaria
gregari_@abv.bg

Svilen Spirdonov
Logictic and Technology Faculty
Vasil Levski National Military University
Veliko Tarnovo, Bulgaria
svilen_spirdonov82@abv.bg

***Abstract* — In today's digitalized world devastated by natural disasters, accidents and catastrophes, the issue of using software applications for the purpose of monitoring and prevention of areas with a high risk of disasters and catastrophes is gaining increasing importance. The purpose of the study is to analyze the regulatory documents regulating critical infrastructure sites and activities for their identification, reporting and protection. The article presents the relationship between the national legislation of the Republic of Bulgaria and the legislation of the European Union regarding the risks of disasters and catastrophes. Using the methods of scientific research as a systematic and scientific analysis, a review of the regulatory documents regulating the protection of critical infrastructure and the possibilities for visualizing the risk of disasters and catastrophes through GIS software applications is carried out. The conclusions of the research show the need for a wider introduction and use of GIS-based software applications with free access, which would allow for the visualization of the risk of disasters in the critical infrastructure sites of the European Union countries. Integrating the collected information into a platform at a European level will enable member states to predict and manage the risks of disasters and catastrophes, which will lead to better advance planning and saving human lives.**

Keywords* — *Critical infrastructure, risk, disasters and accidents, GIS.

I. Introduction

Natural disasters and industrial accidents have become an integral part of human activity and evolution. Despite the attempts to predict them and take measures to prevent them, the damage and suffering they cause are sometimes enormous, and the activities to eliminate their consequences take a long time and cost colossal amounts of money. According to the United Nations Office for the Coordination of Humanitarian Affairs (UNOCHA), nearly 300 million people needed assistance and protection in 2024 due to conflicts, natural disasters, accidents, economic instability, etc. [1]. In addition to the damage and victims of these events, the funds to overcome the consequences amount to billions. According to the analysis of the National Centers for Environmental Information (NCEI), disaster damage in 2024 amounted to approximately $182.7 billion. This total amount places 2024 as the fourth most expensive year in US history after 2017 ($395.9 billion), 2005 ($268.5 billion) and 2022 ($183.6 billion) [2]. When disasters and catastrophes affect the critical infrastructure facilities of a country, the consequences for the population and the country or region become even more severe. This results in the need to take preventive measures to identify critical infrastructure facilities, monitor them and visualize the risks that threaten them.

II. Materials and Methods

This study covers scientific research methods, such as systems analysis – to study the complex set of factors accompanying disasters and accidents and affecting critical infrastructure facilities; scientific analysis – to reveal the leading trends in the development of regulatory documents on the identification and protection of critical infrastructures.

III. Results and Discussion

In 2008, in order to establish a procedure for the identification and designation of European critical

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8492
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

infrastructure and a common approach for assessing the need to improve its protection among the Member States in the European Union, Directive 2008/114/EC [3] of the Council of the European Union on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection within their national borders was adopted. With the introduction of the Directive, basic concepts were formulated such as:

'critical infrastructure' – an element, system or parts thereof located in the Member States which are essential for the maintenance of vital public functions, health, safety, security, economic or social well-being of the population, and whose disruption or destruction would have significant consequences in the given Member State as a result of the impossibility of maintaining these functions;

'European Critical Infrastructures' or 'ECIs' – critical infrastructures located in Member States, the disruption or destruction of which would have significant consequences for two or more Member States. The significance of the consequences is assessed according to cross-sectoral criteria, which also include the consequences of cross-sectoral dependencies on other types of infrastructure;

'risk analysis' – taking into account the relevant scenarios for action under different threats in order to assess the vulnerability and the potential consequences of the disruption or destruction of a critical infrastructure.

The concepts thus formulated and adopted allow for a common understanding between Member States on critical infrastructures and the risks that threaten them. The Directive defines the sectoral and cross-sectoral criteria for establishing ECIs.

The cross-sectoral criteria include: potential number of victims (deaths or injuries); economic consequences (loss and/or deterioration of products or services, including for the environment); societal consequences (for public trust, physical suffering and disruption of daily life; including loss of essential services). The boundaries of the relevant cross-sectoral criteria are determined by the Member States on the basis of the seriousness of the consequences of the disruption or destruction of the given infrastructure in each specific case.

Sectoral criteria take into account the characteristics of the individual sectors with ECIs. The sectors envisaged in the directive are only two – energy (including infrastructures and facilities for the production and transmission of electricity, oil and gas) and transport (road, rail, air, river and maritime).

Based on Directive 2008/114/EC, each Member State should harmonize its national legislation and develop the relevant regulations for the identification, designation and protection of ECIs and their territory. As an EU Member State, the Republic of Bulgaria brought its national legislation into line with the requirements of Directive 2008/114/EC by adopting the Disaster Protection Act [4], and later two regulations – 'Regulation on the procedure, manner and competent authorities for the identification of critical infrastructures and their sites and risk assessment for them' [5] and 'Regulation on the procedure for the identification and designation of European critical infrastructures in the Republic of Bulgaria and measures for their protection' [6].

According to the Disaster Protection Act, it is necessary to carry out preventive activities in order to reduce the risk of disasters, which also include the identification of critical infrastructures and their sites and risk assessment for them, and the specified activities are implemented under a regulation of the Council of Ministers. As for the establishment of a potential European Critical Infrastructure (ECI) on the territory of the Republic of Bulgaria, it is carried out by the relevant minister [4]. Updating of the information in relation to the identification and designation of ECI is carried out periodically every two years by submitting it to the European Commission. The two regulations [5], [6] determine the procedure and responsibilities of the competent authorities for the identification, designation and risk assessment of national and European critical infrastructures and their sites, which will facilitate the adoption of measures to reduce the risk of disasters and protect the population.

The Council of Ministers' Decree № 181 of 20 July 2009 [7] defines the strategic sites and activities that are important for the national security of the Republic of Bulgaria and that are part of the critical infrastructure. 14 sectors are specified, each of which includes the relevant strategic activities and sites:

- Sector 'Agriculture, Food Production and Safety';
- Sector 'Ecology';
- Sector 'Water Resources';
- Sector 'Healthcare';
- Sector 'Energy';
- Sector 'Transport';
- Sector 'Telecommunications and Information';
- Sector 'Government';
- Sector 'Finance';
- Sector 'Education, Science and Technology';
- Sector 'Strategic Objects and Activities of the Ministry of Interior';
- Sector 'Strategic Objects and Activities of the Ministry of Defense';
- Sector 'Strategic Objects and Activities of the National Intelligence Service';
- Sector 'Strategic Objects and Activities of the National Security State Agency.

Decree №181 also defines the obligations of the heads of specific ministries and departments for the implementation of measures for the protection of strategic activities and sites, including the financing of these measures. In 2019, with the onset of the COVID-19 epidemic, a review of Directive 2008/114/EC was carried out, which established that due to the increasingly interconnected and cross-border nature of activities using critical infrastructures, protective measures related only to

individual assets are not sufficient to prevent the occurrence of all types of violations. In order to better account for risks, better define and ensure more consistently the role and obligations of critical entities as providers of services essential for the functioning of the European Union and the resilience of critical entities, Directive (EU) 2022/2557 [8] of 14 December 2022 on the resilience of critical entities was adopted, which repeals Council Directive 2008/114/EC. Directive 2022/2557 provides for obligations on Member States to take specific measures to ensure the uninterrupted provision of services that are significant for the maintenance of essential societal functions or economic activities of the Union. In addition, the document sets out obligations on critical entities responsible for critical infrastructures, and these obligations are aimed at increasing their resilience and their ability to provide services to the internal market. Given the increasing interdependencies between infrastructures and sectors as a result of the increasingly complex cross-border interdependencies in the European Union service provision network, in addition to the existing two sectors, energy and transport, 10 (ten) more sectors with their associated sub-sectors were identified as follows: banking; drinking water, wastewater; food production, processing and distribution; healthcare; space; public administration, financial market infrastructure and digital infrastructure. It is the obligation of each Member State to harmonize its national legislation with the requirements of the Directive by 17 July 2026 and to identify the critical entities for the above-mentioned sectors with their associated sub-sectors.

The review of the regulatory framework of the European Union and the Republic of Bulgaria gives reason to conclude that in recent years, a large number of documents have been adopted regulating critical infrastructure sites, providing guidelines for assessing the risk in them and taking measures to minimize it. This contributes to the harmonization of the national legislation of the member states with that of the European Union. However, there are still not enough software applications generally available to citizens-non-specialists which would allow for the visualization of the risk of disasters and accidents in critical infrastructure sites, especially in populated areas and in their vicinity where there is a large population potentially threatened by specific risks. One of the tools for visualization and monitoring of the risk of disasters and catastrophes, which is increasingly being used in this direction, are various platforms based on Geographic Information Systems.

In recent years, a large number of software based on GIS have been developed and introduced. They have become increasingly used to visualize and monitor areas of disasters and catastrophes, so we will examine their development and application for visualizing risk in critical infrastructure facilities.

A geographic information system is a system that integrates software and hardware for storing, managing, analyzing, visualizing, and sharing geographically-based information (Fig. 1).

These systems integrate specific information with a specific area on a map, linking location data with all kinds of descriptive information. GIS allows users to create interactive queries, analyze spatial information, collect and edit data, maps, and visualize the results of all these activities.

GIS has a wide range of applications, and can be used for engineering design, scientific research, resource management, environmental impact assessment, urban planning, telecommunications, mapping, forensic analysis, historical research, marketing research, and logistics planning.

The origins of GIS date back thousands of years when people painted images of the animals they hunted on cave walls. These drawings were maps of routes and migration paths of animals. One of the earliest successful applications of GIS was in 1854, when John Snow, an epidemiologist and physician, was able to identify a pumping station as the source of a cholera epidemic in London by using spatial analysis.

The founder of modern GIS is considered to be Dr. Roger Tomlinson [9]. In 1962, he created the Canadian Geographic Information System, developed by the federal Department of Forestry and Rural Development in Ottawa, Canada. The system is used to store, analyze, and process land data in rural Canada by mapping information on soils, agriculture, recreation, wildlife, and forestry on maps at a scale of 1:50,000.

Increasingly, GIS-based applications have developed the concept of overlaying different mapped features on top of each other to determine patterns and causes of spatial phenomena (See Figure 2).

In the early 1980s, companies such as M&S Computing (later Intergraph), Environmental Systems Research Institute (ESRI), and CARIS began offering services as GIS software providers, incorporating many of the features of the Canadian GIS, combining a first-generation approach to separating spatial and attribute information with a second-generation approach to organizing attribute data into database structures. More of the software's usability features were developed primarily in a graphical manner with a user-friendly

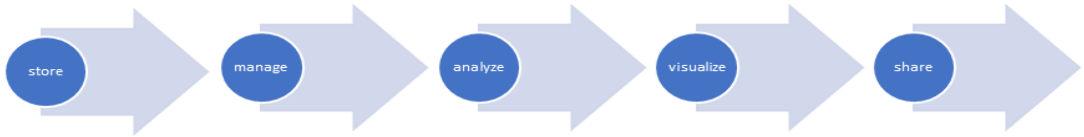


Fig. 1. Geographic information system, presented as software and hardware for storing, managing, analyzing, visualizing, and sharing geographically oriented information.

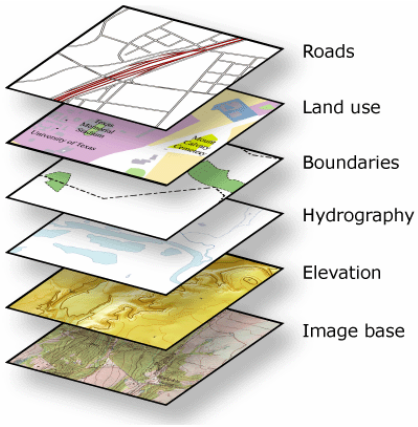


Fig. 2. The following figure illustrates how geographical elements are portrayed in maps through a series of map layers (sfr. ESRI)

Graphical User Interface (GUI) that provided the ability to sort, select, extract, reclassify, reproject, and display data based on complex geographic, topological, and statistical criteria. At the same time, the development of a public-use GIS began at the United States Army Engineering Research Laboratory (USA-CERL) in Champaign, Illinois, a branch of the United States Army Corps of Engineers. The development was provided to meet the United States Army's need for software for land management and environmental planning.

Gradually, GIS applications began to be developed by many private companies, the most widely used of which are: ESRI, GRAM++ GIS, Autodesk, Cadcorp, Intergraph, ERDAS IMAGINE, SuperGeo, SuperMap GIS, IDRISI, MapInfo, MapPoint, Caliper, Pictometry, Black Coral Inc, STAR-APIC, CARIS (Computer Aided Resource Information System), GMS, Manifold System, Oracle Spatial, Safe Software, Smallworld, TatukGIS, Axpand.

One of the applications of GIS is risk management in critical infrastructure areas. Risk management through GIS-based applications is a complex, interdisciplinary field involving computer science, mathematics, statistics, finance, and management [10].

Risk management itself is a process containing the steps of identifying, assessing and treating risks [11]. Risk identification is a complex activity that includes an analysis of the sources and threats of a negative event, the probability of achieving objectives and the occurrence of certain scenarios. Then, based on the identification, risks are assessed in terms of their potential severity of losses and casualties and the probability of the occurrence of the risk events themselves. The final stage of risk management – treatment, includes taking measures to avoid (also known as elimination), reduce (also known as mitigation), assume or transfer risks.

Risk management in complex systems, such as critical infrastructures, which consist of multi-component geographical areas, understanding all the factors involved in a risk situation, is a difficult process. For this reason, risk assessment approaches require taking into account all social, economic, cultural and political aspects in order to determine the vulnerability, resilience and response capacity of the specific system against various threats.

According to some authors, the two main challenges for risk management and resilience of critical infrastructure are the interconnectedness between infrastructures and the multi-actor relationships in which they operate [12]. For this reason, they should be considered as a system in which changes in the state of one of the elements of the system lead to a change in the state of the entire system.

Of great importance for the assessment of the risk of natural disasters or industrial accidents is that they depend on the location, and in many cases, there is sufficient historical information which includes specific data on previous such events (for example, previous earthquakes, floods, fires and potential damages). For the needs of risk assessment, mathematical models are usually prepared in order to establish the probability of a given event occurring with a certain degree of intensity at a given location. The main limitation of this type of approach is that risk necessarily involves uncertainty, and it is necessary to make realistic hypotheses about possible future scenarios.

Once the risk assessment for the occurrence of a specific disaster or accident in critical infrastructure sites is prepared, they are visualized on maps by linking the data about the event to the specific geographical terrain. In this way, GIS technologies visualize the identified risks, the affected areas and the potential damages that can be caused. Presented in this way, spatial information can visualize

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8492
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

relationships, patterns and trends that would not be noticeable otherwise. In a previous study [13], the possibilities of using GIS were discussed, presenting an initial stage of the development of a platform for visualizing the level of risk from industrial accidents or natural disasters in individual zones and regions of critical infrastructure sites using a geographic information system (GIS).

Risk assessment in critical infrastructure sites can be considered as a set of two main components – hazard and vulnerability [14]. Hazard is a measure of the physical intensity of the threat at a given location and the associated probabilities of these intensities, depending on the location (e.g. a location surrounded by seismic faults, near the shore of a water basin, mountainous terrain, etc.). Vulnerability is a measure of the damage that the hazard can cause to the critical infrastructure under study and/or its objects (e.g. in urban areas damage to infrastructure, communications and service provision). The synthesis of these data, presented on a map with the spatial relationships between natural or anthropogenic factors (earthquake, landslide, industrial accident, physical or logical attacks) and the elements at risk (people, buildings, infrastructure), represented through the use of GIS tools, can facilitate crisis response planning and taking preventive measures to protect critical infrastructures.

IV. Conclusions

GIS applications for visualizing risk in critical infrastructure facilities provide a wide range of opportunities for unifying and visualizing information on potential risks from disasters and accidents that could lead to disruption of normal life in society, cessation of essential services, human casualties, and large-scale damage. Free access to these data and their rapid use could significantly facilitate the preliminary planning of activities to minimize the identified risks in critical infrastructures, assessment of potential damage and casualties. This requires the implementation and use of open access GIS software applications for visualizing and assessing the risk of disasters occurring in critical infrastructure facilities not only at the national but also at the European level, using a unified system for their forecasting and management.

V. Acknowledgments

The publication of the article was financed with funds provided by the National Security and Defence Science Program, approved by Decision No. 171/21.10.2021 of the Council of Ministers of the Republic of Bulgaria.

References

[1] Sevil Omer, Aubrey Leasure, 11 Worst Disasters of 2024, https://www.wvi.org/worst-disasters, [Accessed: 18 Feb 2025]

[2] B.Adam, Smith, 2024: An active year of U.S. billion-dollar weather and climate disasters, 10 January 2025, https://www.climate.gov/news-features/blogs/beyond-data/2024-active-year-us-billion-dollar-weather-and-climate-disasters, [Accessed: 18 Feb 2025]

[3] Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union OJ L 345, 23 December 2008, http://data.europa.eu/eli/dir/2008/114/oj, [Accessed: 18 Feb 2025]

[4] Disaster Protection Act, Promulgated in the State Gazette, issue 102 of 19 December 2006, amended and supplemented in the State Gazette, issue 60 of 7 July 2020

[5] Regulation on the procedure, manner and competent authorities for the identification of critical infrastructures and their sites and risk assessment for them In force since 23 October 2012, Adopted by Council of Ministers' Decree № 256 of 17 October 2012, Promulgated in the State Gazette, issue 81 of 23 October 2012, amended and supplemented in the State Gazette, issue 19 of 26 February 2013, amended in the State Gazette, issue 27 of 5 April 2016

[6] Regulation on the procedure for the identification and designation of European critical infrastructures in the Republic of Bulgaria and measures for their protection Adopted by Council of Ministers' Decree № 38 of 18 February 2013. Promulgated in the State Gazette, issue 19 of 26 February 2013.

[7] Decree of the Council of Ministers №181 of 20 July 2009 on the designation of strategic sites and activities of importance for national security, Promulgated in the State Gazette, issue 59 of 28 July 2009, supplemented, issue 71 of 13 September 2011, in force from 13 September 2011, issue 77 of 4 October 2011, amended and supplemented, issue 33 of 20 April 2021, in force from 20 April 2021

[8] Directive (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, Official Journal of the European Union OB L 333, 27 December 2022, http://data.europa.eu/eli/dir/2022/2557/oj, [Accessed: 18 Feb 2025]

[9] D.Pant, M. Kumar, S. Goyal, Fundamentals of GIS, Department of Sensing and GIS School of Earth and Environment Science Uttarakhand Open University Haldwani (Nainital), GIS-503/DGIS-503/CGIS-503, Published By: Uttarakhand Open University, Haldwani, Nainital-263139 , ISBN No.: 978-93-90845-49-1, Edition First, 2021, https://www.uou.ac.in/sites/default/files/slm/GIS-503.pdf, [Accessed: 20 Feb 2025]

[10] J.Stanik, and M. Kiedrowicz, "Risk In Gis Systems", GIS Odyssey Journal, 2022, 2(1), 39–56. https://doi.org/10.57599/gisoj.2022.2.1.39

[11] N. Dimitrov, Security Risk Management in the QUAZAR Competence Center, Nikola Vaptsarov Naval Academy, Varna, 2022, ISBN 978-619-7428-86-5 (print), ISBN 978-619-7428-87-2 (e-book), DOI: 10.13140/RG.2.2.31640.78089

[12] B. Arvidsson, J. Johansson, N. Guldåker, Critical infrastructure, geographical information science and risk governance: A systematic cross-field review. Volume 213, 2021, 107741, ISSN 0951-8320, https://doi.org/10.1016/j.ress.2021.107741

[13] G. Grigor, S. Stefanov, and S. Spirdonov. 'Use of a GIS System to Visualize the Levels of Risk in the Areas of Critical Infrastructure Objects.' Information & Security 55.1 (2024): 55-62. ISSN 0861-5160 (print), ISSN 1314-2119 (online), https://doi.org/10.11610/isij.5521

[14] M. Peggion, A. Bernardini, M. Masera, Geographic Information System and Risk Assessment, European Commission, Joint Research Centre, Institute for the Protection and Security of the Citizen, January 2008, ISSN 1018-5593

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 103-110

Cybersecurity in Smart Cities: A Review of Theoretical Models, Emerging Threats, and Defence Strategies

Genadiy Gospodinov
Computer science department
ULSIT
Sofia, Bulgaria
g.gospodinov@unibit.bg

Lyubomir Gotsev
Computer science department
ULSIT
Sofia, Bulgaria
l.gotsev@unibit.bg

Tamara Ristovska
Computer science department
ULSIT
Sofia, Bulgaria
t.ristovska@unibit.bg

Svetlana Syarova
Computer science department
ULSIT
Sofia, Bulgaria
s.syarova@unibit.bg

Viktoriya Angelova
Computer science department
ULSIT
Sofia, Bulgaria
v.angelova@unibit.bg

***Abstract*—Smart cities represent a new paradigm in urban development, integrating advanced information and communication technologies (ICT) to optimize infrastructure, improve public services, and enhance the quality of life for citizens. However, the increasing interconnectivity of urban systems exposes these cities to significant cybersecurity risks, including data breaches, service disruptions, and infrastructure sabotage. This paper presents a systematic literature review of the theoretical approaches to cybersecurity in smart cities, analyzing their strengths, limitations, and applicability in real-world scenarios. The study categorizes the existing frameworks into three primary groups: classical models, such as the CIA triad and Perimeter-based Security; system-oriented models, like Complex Systems Theory and Game Theory; and innovative models, including Blockchain-based Security and Zero Trust Architecture. The analysis indicates that classical models provide a solid foundation for information security but struggle to address the dynamic and decentralized nature of modern smart city environments. System-oriented models offer improved adaptability, while innovative models demonstrate high efficiency in protecting critical data, albeit with challenges related to implementation complexity and resource requirements. The paper identifies key gaps in the literature, such as the insufficient integration of AI-driven risk assessment techniques and the lack of unified regulatory frameworks across different regions. As a contribution, the study proposes a novel conceptual framework that combines principles from Game Theory, Complex Systems Theory, and Blockchain technology to enhance the resilience of smart city infrastructures. This framework emphasizes proactive risk management through real-time data analysis and adaptive security protocols. The findings of this study provide valuable insights for policymakers, city planners, and cybersecurity researchers, highlighting the need for continued exploration of interdisciplinary approaches to safeguarding the digital backbone of future cities.**

Keywords*— *cybersecurity, smart cities, theoretical models, defence strategies

I. Introduction

The rapid evolution of smart cities has transformed urban environments into interconnected ecosystems driven by Internet of Things (IoT) devices, artificial intelligence (AI), big data, and cloud computing. These technological advancements have enabled efficient resource management, real-time traffic control, energy optimization, and smart governance. However, as the reliance on digital infrastructure grows, so do the cybersecurity risks associated with data breaches, IoT vulnerabilities, ransomware attacks, and cyber-physical system intrusions[1]. The need for robust cybersecurity frameworks has become more critical than ever to ensure the safety and resilience of smart city infrastructures [2].

Smart city cybersecurity involves securing complex, interconnected digital ecosystems that include IoT networks, cloud services, and AI-driven decision-making systems. Various cybersecurity frameworks have been proposed to enhance threat detection, risk mitigation, and

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8496
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

data privacy in these environments. For instance, the National Institute of Standards and Technology (NIST) Cybersecurity Framework provides a risk-based approach for protecting smart city infrastructure by emphasizing continuous monitoring, real-time threat intelligence, and incident response strategies [3]. Additionally, Zero Trust Security Models are being widely adopted to enforce strict identity verification, micro-segmentation, and least-privilege access policies to prevent unauthorized access and lateral movement within urban networks [4].

A study by Zhou et al [5] highlights the growing importance of machine learning-powered security solutions for smart cities, which enable real-time anomaly detection, automated threat response, and adaptive defense mechanisms. These AI-driven systems continuously analyze network traffic, user behavior, and IoT device activity to identify potential cyber threats before they escalate [6]. Moreover, blockchain technology has emerged as a promising solution for securing digital identities, financial transactions, and supply chains in smart cities. Research by Khatoon & Riaz [7] demonstrates that blockchain-powered authentication mechanisms can significantly reduce identity fraud and data manipulation risks, making them ideal for e-governance, healthcare, and energy distribution systems.

Despite advancements in cybersecurity frameworks, smart cities remain highly vulnerable to cyberattacks due to the vast attack surface created by millions of interconnected IoT devices [8]. Some of the most common threats include ransomware, IoT-based malware, phishing attacks, Distributed Denial of Service (DDoS) attacks, and nation-state cyber espionage [9]. For example, AI-powered ransomware has become a growing concern, as cybercriminals leverage machine learning algorithms to enhance attack efficiency, evade detection, and automate exploit distribution [10].

Another significant cybersecurity challenge is data privacy and regulatory compliance. Smart cities collect vast amounts of citizen data, including biometric information, geolocation data, and financial records, raising concerns about unauthorized access, mass surveillance, and privacy breaches [11]. Governments and municipal authorities must ensure that cybersecurity measures comply with global data protection laws, such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States [1]. Failure to comply with these regulations can lead to severe legal consequences, financial penalties, and reputational damage for city administrators.

This study aims to provide a comprehensive review of existing cybersecurity frameworks, challenges, and risk mitigation strategies for smart cities. The research will explore:

- Current cybersecurity threats and their impact on urban infrastructures.
- Emerging security solutions, including AI-driven threat detection, blockchain-based authentication, and quantum encryption.
- Regulatory challenges and the role of international cybersecurity standards in smart city governance.
- Future research directions, focusing on federated learning, decentralized security architectures, and adaptive cyber defense mechanisms.

By analyzing these key areas, this study will contribute to the development of resilient, scalable, and future-proof cybersecurity models tailored for smart cities. Additionally, the research findings will serve as a valuable resource for municipal decision-makers, policymakers, cybersecurity experts, and technology developers aiming to enhance urban cybersecurity resilience.

The pyramid model shown on Fig. 1 illustrates the hierarchical approach to cybersecurity in smart cities, structured from low-level security protections to advanced AI-driven defense mechanisms:

- IoT Security (Base Layer): The foundation of smart city cybersecurity, focused on securing IoT devices, sensors, and network endpoints from cyber threats. Weak authentication and poor encryption at this level can lead to widespread vulnerabilities.
- Network Security: Ensures secure data transmission between IoT devices, cloud platforms, and municipal control centers. This includes firewalls, secure communication protocols, and intrusion detection systems.
- Cloud Security: Smart cities store and process vast amounts of citizen data in cloud-based infrastructures. Strong access controls, encryption, and compliance measures help mitigate risks like data breaches.
- AI-Driven Monitoring: AI-based threat detection systems continuously monitor smart city infrastructure, identifying anomalous patterns and preventing cyber threats in real time.
- Data Encryption (Top Layer): The final and most critical layer, ensuring that all sensitive information remains secure, even in case of a system breach. Quantum-safe encryption is emerging as a long-term solution for protecting municipal data.

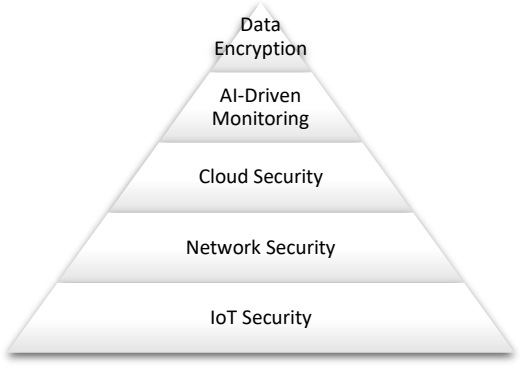


Fig. 1. Smart City Cybersecurity Layers (Pyramid model).

II. Materials and Methods

This study adopts a systematic literature review (SLR) methodology to comprehensively examine cybersecurity frameworks for smart cities. Given the complexity and evolving nature of cybersecurity threats, conducting an SLR ensures a rigorous, structured, and replicable approach to identifying, analyzing, and synthesizing existing research in this domain [12]. Unlike traditional literature reviews, which may be narrative or selective, an SLR follows a predefined search strategy, inclusion and exclusion criteria, and a structured data extraction process, ensuring that findings are objective, transparent, and methodologically sound. This methodology is particularly useful in cybersecurity research, as it allows for the identification of patterns, knowledge gaps, and emerging security strategies while minimizing the risks of bias and incompleteness.

To ensure high methodological standards, this study follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, which are widely recognized for conducting transparent and replicable systematic reviews [13]. The PRISMA framework consists of four key phases: (1) Identification, where relevant research papers are located through comprehensive database searches; (2) Screening, where duplicate or irrelevant studies are removed based on title and abstract reviews; (3) Eligibility Assessment, where full-text articles are evaluated against predefined inclusion criteria; and (4) Inclusion, where only the most relevant, high-quality studies are selected for in-depth analysis. This structured process ensures that the findings presented in this study are based on verified, peer-reviewed sources and contribute meaningfully to the understanding of cybersecurity frameworks in smart cities.

The selection of an SLR as the research methodology is particularly justified by the rapid evolution of cyber threats and security solutions in urban environments. Given the increasing integration of AI, IoT, and cloud computing in smart city infrastructure, cyber risks are constantly changing, requiring a comprehensive assessment of multiple cybersecurity models to identify the most effective strategies [14]. This study, therefore, aims to systematically evaluate existing cybersecurity frameworks, critically analyze their effectiveness, and provide recommendations for future research and implementation strategies.

To conduct a comprehensive and unbiased review, this study relies on multiple academic databases and digital libraries that specialize in cybersecurity, information technology, and smart city governance. The primary databases searched include IEEE Xplore, ACM Digital Library, ScienceDirect (Elsevier), SpringerLink, and Google Scholar, among others, each of which is known for its extensive collection of peer-reviewed articles, conference proceedings, and technical reports. These databases provide access to state-of-the-art research on cybersecurity models, risk mitigation strategies, and emerging security technologies, ensuring that this study captures a broad and interdisciplinary perspective on smart city cybersecurity.

The search strategy employed a combination of keywords and Boolean operators to refine search results and identify the most relevant studies. The following search queries were used across all databases:

- "Cybersecurity frameworks AND smart cities"
- "Systematic literature review AND cybersecurity models"
- "Game Theory AND cybersecurity in urban infrastructures"
- "Zero Trust AND smart cities cybersecurity"
- "Blockchain security AND IoT-based smart cities"
- "Smart data models AND Cybersecurity"

By using Boolean operators (AND, OR, NOT), the search process was optimized to retrieve studies that focused specifically on cybersecurity in smart cities while filtering out research that was too general or unrelated to urban infrastructures. Additional manual searches were conducted using citation tracking, allowing the identification of seminal works that were frequently referenced in cybersecurity literature.

To maintain the relevance and applicability of the findings, several filters were applied during the search process. Only studies published between 2019 and 2024 were included to ensure that the analysis reflects the latest advancements and challenges in cybersecurity for smart cities. Additionally, only English-language publications were considered, as English is the dominant language for cybersecurity research and technical documentation. Studies that were not peer-reviewed, such as industry white papers, blog posts, and government reports, were excluded to maintain the academic rigor of this study, except the case it was quite helpful in providing more information and clearance in a specific topic.

Following the search and filtering process, duplicate studies were removed, and the remaining articles underwent a title, abstract, and full-text screening to determine their relevance. This multi-step process ensured that only the most credible and high-impact research papers were included in the final analysis, allowing for a robust

and evidence-based discussion of cybersecurity models in smart cities.

To ensure the selection of only the most relevant and high-quality research, this study applies strict inclusion and exclusion criteria during the article selection process. The inclusion criteria specify that only studies that propose, evaluate, or compare cybersecurity frameworks in smart cities are considered. Studies must be published in peer-reviewed journals or conference proceedings between 2019 and 2024 to ensure that they reflect recent advancements in cybersecurity strategies. Additionally, articles must explicitly address Game Theory-based security models, Zero Trust Architecture, Blockchain-based security, or AI-driven cybersecurity solutions within the context of smart cities. Empirical studies, systematic reviews, and meta-analyses that provide quantitative or qualitative evaluations of cybersecurity threats and solutions were prioritized.

In contrast, the exclusion criteria filter out studies that focus on general cybersecurity without specific applications to smart cities. Non-peer-reviewed sources, such as industry reports, blogs, and unpublished manuscripts, were excluded to maintain the academic integrity of the study. Additionally, studies published before 2019 were not included unless they presented fundamental cybersecurity models that remain widely referenced in recent literature. Articles that were redundant or covered similar topics without offering new insights were also removed to avoid duplication in the analysis.

Following the application of the inclusion and exclusion criteria, 23 peer-reviewed studies were selected for final analysis. Each study was systematically analyzed and coded based on the following key parameters: publication year, cybersecurity model discussed, cyber threats addressed, effectiveness of the proposed framework, and identified challenges in implementation. This structured data extraction process enabled a comparative analysis of cybersecurity models, allowing for the identification of common themes, emerging trends, and critical gaps in the research.

The qualitative synthesis of data follows thematic analysis principles, grouping findings into major cybersecurity categories, such as preventive security measures, predictive threat modelling, decentralized authentication mechanisms, and AI-driven security solutions [14]. By organizing the data in this manner, the study presents a clear and systematic overview of existing cybersecurity frameworks, highlighting their strengths, weaknesses, and applicability to smart city infrastructures.

III. Results and Discussion

The development of smart cities has led to rapid urban digitalization, integrating advanced technologies such as Internet of Things (IoT) devices, artificial intelligence (AI), cloud computing, and big data analytics to improve efficiency in urban management. However, these interconnected systems introduce significant cybersecurity risks, exposing municipalities to data breaches, ransomware attacks, infrastructure sabotage, and surveillance risks [15]. As the number of connected devices in smart city ecosystems grows, so does the attack surface available to cybercriminals[16]. With city operations relying heavily on autonomous control systems, a single cyberattack has the potential to disrupt critical services such as energy distribution, traffic control, healthcare, and public safety [17].

One of the most critical cybersecurity risks in smart cities is the vulnerability of IoT networks [18], [19]. IoT devices—including smart meters, connected surveillance cameras, smart traffic systems, and environmental sensors—often have inadequate security configurations, making them easy targets for botnets, malware infections, and unauthorized access [20]. The Mirai botnet attack of 2016 remains one of the most well-known cases, where hackers exploited weak security settings in IoT devices to create a massive Distributed Denial-of-Service (DDoS) attack, crippling major internet services [21]. More recently, researchers have identified AI-enhanced botnets, which use machine learning algorithms to optimize attack patterns and evade detection mechanisms, posing an even greater threat to smart city infrastructures [4], [22].

Another growing concern is ransomware attacks targeting municipal governments and essential public services. In these attacks, hackers encrypt critical data and demand ransom payments in exchange for restoring access. One of the most severe incidents occurred in 2019, when Baltimore's municipal systems were paralyzed by the RobbinHood ransomware, disrupting emergency services, water billing, and property transactions for weeks, resulting in over $18 million in damages [23]. In recent years, ransomware groups have increasingly leveraged AI-powered automation, making their attacks faster, more targeted, and harder to detect [21]. Studies show that municipal governments are now among the top targets of ransomware campaigns, as they often lack robust cybersecurity defences and are willing to pay large ransoms to restore critical operations [24].

Beyond ransomware, smart cities also face serious threats from data breaches and mass surveillance risks. Municipal systems collect vast amounts of sensitive citizen data, including personal identification information, biometric data, and financial transactions, making them attractive targets for cybercriminals and intelligence agencies [25], [26]. The Singapore Health Data Breach of 2018 remains one of the most severe cybersecurity incidents in urban history, where 1.5 million patient records, including those of high-profile officials, were compromised due to vulnerabilities in the nation's health database. Similarly, the adoption of AI-driven facial recognition and behavioural monitoring systems in smart cities raises concerns over mass surveillance, data misuse, and potential civil rights violations [27].

A particularly alarming category of cyber threats in smart cities involves nation-state cyber espionage and cyber-physical system (CPS) attacks. State-sponsored hacking groups have been linked to sophisticated cyberattacks on national infrastructure, including power

grids, transportation networks, and emergency response systems [23]. One of the most well-documented cases is the Kyiv power grid attack of 2016, in which Russian-backed hackers compromised Ukraine's power infrastructure, leaving thousands without electricity for hours [28]. The increasing geopolitical tension in cyber warfare suggests that future conflicts may involve large-scale cyberattacks targeting urban infrastructure, reinforcing the need for advanced cybersecurity frameworks in smart cities [29].

TABLE I CYBERSECURITY THREAT TYPES IN SMART CITIES

Threat Type	Impact	Real-World Example
Iot Vulnerabilities	Unauthorized access, botnet attacks	Mirai Botnet (2016)
Ransomware	Data encryption, service disruption	Baltimore Ransomware Attack (2019)
Data Breaches	Identity theft, financial losses	Singapore Health Data Breach (2018)
Nation-State Attacks	Infrastructure sabotage, power grid hacking	Kyiv Power Grid Attack (2016)
AI-Powered Cyber Attacks	Automated hacking, adversarial AI manipulation	AI-enhanced Phishing Attacks (2023)

Table I categorizes major cybersecurity threats in smart cities, outlining their impact on urban infrastructure and providing real-world cases to illustrate the severity of these threats.

To counteract these growing cyber threats, smart cities are turning to AI-driven security solutions to enhance threat detection, predictive analytics, and automated response mechanisms. AI-based Intrusion Detection Systems (IDS) continuously monitor network traffic, system logs, and user behaviour, identifying irregular patterns that could signal cyberattacks [11]. These AI-enhanced security systems are capable of detecting anomalies in real time, allowing municipalities to prevent cyber threats before they escalate [30].

A major success story in AI-driven cybersecurity can be seen in Singapore's smart city defence initiative, where AI-powered risk assessment tools have been deployed to protect government infrastructure from cyberattacks [20]. AI-driven threat intelligence platforms used in New York City's digital security systems have reduced incident response times by 60%, demonstrating the effectiveness of machine learning-based cybersecurity strategies [10].

Despite its advantages, AI-driven cybersecurity also introduces new risks. One emerging concern is adversarial AI attacks, where hackers manipulate AI models by feeding them deceptive data, tricking the system into misclassifying threats [27]. Additionally, over-reliance on AI-powered security tools raises questions about false positives, algorithmic bias, and privacy concerns in urban cybersecurity [7].

To address these challenges, federated learning-based AI security models have been proposed, allowing smart city AI models to be trained across multiple decentralized nodes without sharing raw data [31].

Researchers are also exploring the integration of AI and blockchain security solutions, where tamper-proof blockchain ledgers enhance AI-powered threat detection and authentication mechanisms [29].

Table II compares five key cybersecurity solutions, highlighting their advantages, challenges, and practical use cases in smart city environments.

TABLE II COMPARATIVE ANALYSIS OF CYBERSECURITY SOLUTIONS

Cybersecurity Solution	Strengths	Limitations	Application in Smart Cities
AI-Based Intrusion Detection	Real-time threat monitoring, automated response	Vulnerable to adversarial AI attacks	Smart surveillance, traffic monitoring
Blockchain Authentication	Decentralized, tamper-proof identity verification	High computational cost, scalability issues	Secure citizen IDs, municipal records
Quantum Cryptography	Unbreakable encryption, quantum key distribution	Expensive, still in early development	Securing government communications
Federated Learning Security	Privacy-preserving AI training, decentralized security	Requires significant computing power	AI-driven cybersecurity frameworks
Zero Trust Architecture	Continuous authentication, micro-segmentation	Complex to implement in legacy systems	Enterprise and municipal IT security

Table II compares five key cybersecurity solutions, highlighting their advantages, challenges, and practical use cases in smart city environments.

The research identified that AI-based cybersecurity solutions, blockchain authentication mechanisms and quantum cryptography are among the most promising approaches to mitigating smart city cyber risks [22], [32], [33]. AI and machine learning-powered intrusion detection systems (IDS) have proven effective in identifying real-time cyber threats, with notable success in Singapore's public transit networks and New York City's surveillance infrastructure [34]. Blockchain-based security solutions have also demonstrated robust fraud prevention capabilities, particularly in smart energy grids and digital identity management, with successful implementations in Amsterdam and Dubai [7]. However, despite their potential, challenges such as high computational costs, data

privacy concerns, and scalability limitations continue to hinder the widespread adoption of these technologies [4].

Table III outlines emerging research priorities in smart city cybersecurity, explaining their goals and expected benefits for urban resilience.

TABLE III FUTURE RESEARCH DIRECTIONS IN SMART CITY CYBERSECURITY

Research Focus	Objective	Expected Impact
AI-Driven Cyber Resilience	Develop adaptive, self-healing security models	Improved real-time threat response
Quantum-Safe Encryption	Implement post-quantum cryptography	Future-proof smart city data protection
Privacy-Preserving AI	Enhance AI-driven security without exposing sensitive data	Better compliance with data regulations
Blockchain for IoT Security	Improve decentralized authentication for IoT devices	Stronger protection against IoT cyberattacks
Automated Threat Intelligence	AI-driven early warning systems for cyber threats	Faster attack mitigation and response

IV. CONCLUSION

The rapid development of smart cities has introduced unprecedented challenges in cybersecurity, necessitating the implementation of advanced security measures to protect critical urban infrastructures. This study has provided a comprehensive analysis of cybersecurity threats, existing frameworks, and future research directions for enhancing smart city security. The findings highlight that IoT vulnerabilities, ransomware attacks, data breaches, and cyber-physical threats are among the most pressing risks facing smart cities today. The interconnected nature of smart city technologies increases the attack surface, making traditional perimeter security models inadequate and calling for more proactive, AI-driven security strategies.

A significant challenge remains in the regulatory and compliance landscape for cybersecurity in smart cities. International data protection laws, including GDPR in Europe and CCPA in the United States, impose strict regulations on data processing, storage, and cross-border transfers. While such regulations enhance data privacy, they also create challenges in establishing a standardized cybersecurity framework applicable across different jurisdictions. Additionally, financial constraints prevent many municipal governments, particularly in developing regions, from investing in state-of-the-art cybersecurity infrastructure. These economic barriers highlight the need for public-private partnerships (PPPs) and government-led cybersecurity funding initiatives to ensure that smart cities can afford advanced protection mechanisms.

Future research in smart city cybersecurity must focus on developing more scalable, cost-effective, and proactive defence mechanisms to address emerging cyber threats. One critical area for further investigation is the integration of federated learning in smart city cybersecurity frameworks. Unlike traditional AI models that require centralized data processing, federated learning allows multiple devices and systems to collaboratively train security models without exposing raw data, thereby enhancing privacy protection and real-time threat detection.

Another promising avenue for research is the role of quantum computing in cybersecurity. While quantum encryption technologies such as Quantum Key Distribution (QKD) have already been tested in government communications, their practical application in smart city cybersecurity remains largely unexplored. Future studies should assess the feasibility of quantum-safe encryption algorithms to protect IoT-enabled smart cities from advanced cyber threats.

Moreover, the convergence of blockchain, AI, and IoT in smart city cybersecurity presents opportunities for fully automated, self-healing security frameworks. A decentralized AI-driven security system that leverages blockchain for data integrity, AI for predictive analytics, and IoT for real-time threat monitoring could significantly enhance the resilience of urban infrastructure against cyberattacks. Research should also investigate the ethical and policy implications of AI-driven cybersecurity, ensuring that automated decision-making aligns with data protection laws and privacy regulations.

Another urgent area for future research is cybersecurity awareness and human factor analysis in smart cities. Despite technological advancements, human error remains one of the leading causes of cybersecurity breaches. Future studies should explore the impact of cybersecurity training programs for municipal employees, public awareness initiatives, and the effectiveness of behavioural-based cybersecurity approaches.

Governments and policymakers must adopt a multi-layered approach to strengthen cybersecurity in smart cities. First, standardized cybersecurity policies should be developed to ensure interoperability and regulatory compliance across jurisdictions. Second, governments should promote collaborative cybersecurity frameworks that encourage knowledge sharing between municipalities, research institutions, and private sector stakeholders. Third, investing in cyber resilience programs that focus on real-time threat intelligence sharing, incident response planning, and continuous security assessments is crucial for reducing cyber risks in urban environments.

Lastly, policymakers must prioritize cybersecurity as a core component of smart city planning by integrating security-by-design principles into the development of urban technologies. Future smart city projects should adopt AI-driven penetration testing, blockchain-based digital identity verification, and quantum-safe encryption methods as standard security measures.

Cybersecurity is a critical factor in ensuring the long-term success of smart cities. Without robust security frameworks, urban environments remain vulnerable to cyberattacks, data breaches, and system failures that could disrupt essential services. This study has highlighted the key cybersecurity threats, technological solutions, and policy challenges that must be addressed to safeguard smart cities against future cyber risks. While AI, blockchain, and quantum encryption offer promising solutions, further research is needed to address their limitations, ensure scalability, and develop cost-effective security solutions for urban infrastructure.

As smart cities continue to evolve, cybersecurity must be treated as a fundamental component of urban planning, requiring collaboration between governments, the private sector, and academic researchers. By adopting proactive security frameworks, investing in next-generation cybersecurity technologies, and implementing comprehensive policy measures, cities can enhance their resilience against emerging cyber threats and build a secure, sustainable digital future.

ACKNOWLEDGEMENTS

This paper is supported by:

European Union-NextGenerationEU through the National Recovery and Resilience Plan of the Republic of Bulgaria project № BG-RRP-2.005-0003.

National Science Fund, under project No. BG-175467353-2024-10-0013, contract No. КП-06-М87/5, dated December 6, 2024, with the project title: Artificial Intelligence and Cybersecurity: Navigating the Ethical Challenges.

REFERENCES

[1] M. A. Shaik and P. Sneha, “Revolutionizing Infrastructure Resilience: AI-Driven Predictive Maintenance and Structural Health Monitoring,” Jan. 2025, doi: 10.20944/PREPRINTS202501.0480.V1.

[2] S. T. Hossain, T. Yigitcanlar, K. Nguyen, and Y. Xu, “Cybersecurity in local governments: A systematic review and framework of key challenges,” Urban Governance, Jan. 2025, doi: 10.1016/J.UGJ.2024.12.010.

[3] H. Janicke et al., “Generative AI-Enhanced Cybersecurity Framework for Enterprise Data Privacy Management,” Computers 2025, Vol. 14, Page 55, vol. 14, no. 2, p. 55, Feb. 2025, doi: 10.3390/COMPUTERS14020055.

[4] B. Tandan, P. Vajpayee, and G. Hossain, “Explaining Cyber Risks in Transportaion 5.0: A Data Driven Approach,” 2025 IEEE 4th International Conference on AI in Cybersecurity, ICAIC 2025, 2025, doi: 10.1109/ICAIC63015.2025.10848812.

[5] L. Zhou, A. Gaurav, V. Arya, R. W. Attar, S. Bansal, and A. Alhomoud, “Smart City Electronics Security Using XGBoost with Metaheuristic Algorithms,” IEEE Consumer Electronics Magazine, 2025, doi: 10.1109/MCE.2024.3524998.

[6] K. Achuthan, S. Sankaran, S. Roy, and R. Raman, “Integrating sustainability into cybersecurity: insights from machine learning based topic modeling,” Discover Sustainability, vol. 6, no. 1, Dec. 2025, doi: 10.1007/S43621-024-00754-W.

[7] A. Khatoon and R. Riaz, “Quantum Computing Impacts on Smart City Cybersecurity Through Resilient Defense Framework: Quantum Computing Impacts on Resilient Cybersecurity Frameworks for Smart Cities,” Ubiquitous Technology Journal, vol. 1, no. 1, pp. 23–31, Feb. 2025, doi: 10.71346/UTJ.V1I1.8.

[8] W. A. Jasim et al., “Implications and Transformative Potential of 5G-Enabled M2M Communication for the IoT Landscape”.

[9] F. J. Gallardo-Amores, C. Del-Real, and A. M. Díaz-Fernández, “Assessing urban security and safety smartness: A systematic review of key performance indicators,” IET Smart Cities, vol. 7, no. 1, p. e70000, Jan. 2025, doi: 10.1049/SMC2.70000.

[10] S. Wang, “Challenges and opportunities for developing a smart city based on artificial intelligence,” Applied Innovations in Industrial Management , vol. 5, no. 1, pp. 62–69, Jan. 2025, Accessed: Feb. 24, 2025. [Online]. Available: https://iscihub.com/index.php/AIIM/article/view/35

[11] A. Anitha and T. Haritha, “Blockchain-Based Shielding Framework to Enhance Security in Smart Cities,” Artifcial Intelligence and IoT for Cyber Security Solutions in Smart Cities, pp. 146–165, Jan. 2025, doi: 10.1201/9781003459835-9/BLOCKCHAIN-BASED-SHIELDING-FRAMEWORK-ENHANCE-SECURITY-SMART-CITIES-ANITHA-HARITHA.

[12] **B.**Kitchenham, and S. Charters, Guidelines for Performing Systematic Literature Reviews in Software Engineering, Technical Report EBSE 2007-001, Keele University and Durham University Joint Report. - References - Scientific Research Publishing.”2007. Accessed: Feb. 24, 2025. [Online]. Available: https://www.scirp.org/reference/ReferencesPapers?ReferenceID=1555797

[13] D. Moher et al., “Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement,” PLoS Med, vol. 6, no. 7, Jul. 2009, doi: 10.1371/JOURNAL.PMED.1000097.

[14] A. Gunuganti, “(PDF) Artificial Intelligence and Machine Learning in Cyber-Security.” Accessed: Feb. 24, 2025. [Online]. Available: https://www.researchgate.net/publication/388836506_Artificial_Intelligence_and_Machine_Learning_in_Cyber-Security

[15] N. Ahmad and A. Haile, “(PDF) Smart City Parking: Leveraging AI and IoT for Efficient Space Utilization and Billing.” Accessed: Feb. 25, 2025. [Online]. Available: https://www.researchgate.net/publication/389026841_Smart_City_Parking_Leveraging_AI_and_IoT_for_Efficient_Space_Utilization_and_Billing

[16] T. Zhukabayeva, A. Adamova, N. Karabayev, Y. Mardenov, and D. Satybaldina, “Comprehensive Vulnerability Analysis and Penetration Testing Approaches in Smart City Ecosystems,” 8th International Symposium on Innovative Approaches in Smart Technologies, ISAS 2024 - Proceedings, 2024, doi: 10.1109/ISAS64331.2024.10845637.

[17] A. W, D. R. D. Brabin, K. K. Kumar, and T. Sunitha, “Strengthening security in IoT-based smart cities utilizing cycle-consistent generative adversarial networks for attack detection and secure data transmission,” Peer Peer Netw Appl, vol. 18, no. 2, pp. 1–16, Apr. 2025, doi: 10.1007/S12083-024-01838-0/METRICS.

[18] Y. Aounzou, A. Boulaalam, and F. Kalloubi, “INTERNATIONAL JOURNAL ON SMART SENSING AND INTELLIGENT SYSTEMS Convergence of blockchain, IoT, and machine learning: exploring opportunities and challenges-a systematic review,” vol. 18, 2025, doi: 10.2478/ijssis-2025-0002.

[19] A. Mohammed, “Cybersecurity for Internet of Things (IoT): Vulnerabilities and Protection Strategies,” Innovative Computer Science Journal, Sep. 2021, Accessed: Feb. 26, 2025. [Online]. Available: https://www.academia.edu/127358157/Cybersecurity_for_Internet_of_Things_IoT_Vulnerabilities_and_Protection_Strategies

[20] F. Tahir and M. Rasool, “(PDF) The Role of Artificial Intelligence in Urban Transportation for Smart City

Development and Sustainable Transportation Planning." Accessed: Feb. 25, 2025. [Online]. Available: https://www.researchgate.net/publication/388485734_The_Role_of_Artificial_Intelligence_in_Urban_Transportation_for_Smart_City_Development_and_Sustainable_Transportation_Planning

[21] V. Jain and A. Mitra, "AI Applications in Secure 6G-Enabled Smart City Infrastructure," pp. 175–198, Dec. 2024, doi: 10.4018/979-8-3693-8029-1.CH007.

[22] B. Gul and F. Ertam, "In-vehicle communication cyber security: A comprehensive review of challenges and solutions," Vehicular Communications, vol. 50, p. 100846, Dec. 2024, doi: 10.1016/J.VEHCOM.2024.100846.

[23] S. Hamid and N. Z. Bawany, "Federated Learning for Enhanced Intrusion Detection in Smart City Environments," 2024 18th International Conference on Open Source Systems and Technologies (ICOSST), pp. 1–6, Dec. 2024, doi: 10.1109/ICOSST64562.2024.10871154.

[24] Q. Lyu, S. Liu, and Z. Shang, "Securing Urban Landscape: Cybersecurity Mechanisms for Resilient Smart Cities," IEEE Access, 2024, doi: 10.1109/ACCESS.2024.3522078.

[25] H. Alkhudhayr and H. Ardah, "Mitigating cyberphysical risks in IoT-enabled smart transport infrastructure," Journal of Supercomputing, vol. 81, no. 2, pp. 1–29, Jan. 2025, doi: 10.1007/S11227-025-06948-X/METRICS.

[26] V. Voronkova, V. Nikitenko, V. Marienko, and M. Gramchuk, "Philosophy of Artificial Intelligence Society as the Main Strategy for Increasing National Competitiveness," Laisvalaikio tyrimai, vol. 2, no. 24, pp. 50–63, Dec. 2024, doi: 10.33607/ELT.V2I24.1527.

[27] A. Hyra and F. Premti, "The Double-Edged Sword of AI in Cybersecurity: Boosting Security While Addressing Privacy Risks," Smart Cities and Regional Development (SCRD) Preprints, vol. 1, no. 1, Dec. 2024, Accessed: Feb. 25, 2025. [Online]. Available: https://scrd.eu/index.php/scrd-pp/article/view/583

[28] J. Stanly Jayaprakash, S. Kodati, A. Kanchana, M. Al-Farouni, and R. A C, "An Effective Cyber Security Threat Detection in Smart Cities Using Dueling Deep Q Networks," 2024 4th International Conference on Mobile Networks and Wireless Communications (ICMNWC), pp. 1–5, Dec. 2024, doi: 10.1109/ICMNWC63764.2024.10872116.

[29] M. Alotaibi et al., "Integrating Two-Tier Optimization Algorithm with Convolutional Bi-LSTM Model for Robust Anomaly Detection in Autonomous Vehicles," IEEE Access, 2024, doi: 10.1109/ACCESS.2024.3523539.

[30] W. Shafik, "Artificial Intelligence-Enabled Cybersecurity and Internet of Things Applications in Smart Cities," https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/979-8-3693-8029-1.ch011, pp. 301–334, Jan. 1AD, doi: 10.4018/979-8-3693-8029-1.CH011.

[31] Smita. Sharma, Manikandan. Thirumalaisamy, Balamurugan. Balusamy, and Naveen. Chilamkurti, "Artificial intelligence and IoT for cyber security solutions in smart cities," p. 197, 2025, Accessed: Feb. 25, 2025. [Online]. Available: https://books.google.com/books/about/Artificial_Intelligence_and_IoT_for_Cybe.html?hl=bg&id=zuk5EQAAQBAJ

[32] A. Mccall, "(PDF) Cybersecurity in the Age of AI and IoT: Emerging Threats and Defense Strategies." Accessed: Feb. 26, 2025. [Online]. Available: https://www.researchgate.net/publication/386050391_Cybersecurity_in_the_Age_of_AI_and_IoT_Emerging_Threats_and_Defense_Strategies

[33] A. L. Ahmad, A. A. Danlami, and K. G. Samuel, "(PDF) Blockchain-Empowered Cybersecurity Solutions Across Diverse Application Domains: A Survey." Accessed: Feb. 26, 2025. [Online]. Available: https://www.researchgate.net/publication/387055751_Blockchain-Empowered_Cybersecurity_Solutions_Across_Diverse_Application_Domains_A_Survey

[34] H. P. Joshi and S. A. Sulaiman, "Revolutionizing Smart City Communication: A Secure Framework Using Modern Security Technologies," Asian American Research Letters Journal, vol. 1, no. 10, pp. 48–64, Dec. 2024, doi: 10.5281/361J4S82.

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 111-118

Modern Views in the Analysis and Evaluation of Command and Control Systems

Teodora Georgieva
Rakovski National Defence College
Defense Advanced Research Institute
Sofia, Bulgaria
t.georgieva@rndc.bg

Ivo Radulov
Rakovski National Defence College
Defense Advanced Research Institute
Sofia, Bulgaria
i.radulov@rndc.bg

***Abstract*—The digitalization of the battlefield creates conditions for an unprecedented enlargement in mobility and parallelism of combat operations. The resulting effect is the increased complexity in implementing the command and coordination functions of the command and control (C2) systems. C2 networks, as the communication infrastructure of C2 systems for issuing orders and disseminating information in real time, are a key element for data exchange between commanders, troops and other related organizations. The characteristics and evolutionary behaviour of C2 networks are described by complex hierarchical associations, interwoven communication links, and dynamic changes. It is their complexity that has become the subject of innovative research approaches and created some of the latest scientific products in the field of C2 systems. The research focus in this report is directed at presenting and comparing typological varieties of modern networked C2 approaches – hypernetworks and supernetworks. Hypernetworks are neural networks that generate weights for another neural target network, and are useful in describing C2 networks with complex levels, intertwining connections and dynamic topology. Supernetworks are a networking technique that consolidates multiple smaller networks into a larger one, simplifying routes and reducing their size. The comparison of the particular variations of the theories is carried out in order to identify the areas of application and solved tasks. References to the C2 networks of the C2 systems in the Bulgarian Armed Forces are provided.**

***Keywords*—Command and control systems, command and control networks, hypernetworks, supernetworks.**

I. INTRODUCTION

C2 networks, as the communication infrastructure of C2 systems for issuing orders and disseminating information in real time, are a key element for data exchange between commanders, troops and other related organizations. The characteristics and evolutionary behaviour of C2 networks are described by complex hierarchical associations, interwoven communication links, and dynamic changes.

A. Traditional Network Model

Network models based on graph theory are a powerful tool for solving a lot of practical problems related to optimization and analysis of systems (including C2 systems), where interactions between elements can be represented graphically. Their structure is operationalized by nodes (objects or states in the network) and edges, which represent the connections between vertices. Edges can have weights that denote costs, distances or travel times between connected vertices and allow optimization of the network according to various criteria. Nodes, edges, weights are analysed and visualized by various mathematical algorithms and formulas. Traditional networks usually follow a hierarchical structure, where devices and resources are organized into clearly defined layers and roles. They use standard network protocols, and their management often requires centralized administration and configuration [1, 2].

Despite the wide application of classical network models in command and control (C2) systems, their functioning in this area is accompanied by a number of limitations and shortcomings. Modelling and management of the system are difficult or impossible as the complexity of the network increases or in the presence of dynamic processes. Classical models are unable to reflect the dynamic aspects of real-time interactions, which is essential for effective command and control. Most developments cannot cope with unstructured (incomplete or inaccurate) data, they are unable to integrate different types of data into a single graph model, and do not offer sufficient tools for analysing complex scenarios and relationships. Classical graph models can be too static and inert, as they do not offer enough flexibility to quickly adapt to changing conditions or requirements. The inability to integrate with new technologies, platforms, and services

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8476
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

that contain the potential for improving management and command is another of their limitations [3, 4].

The outlined shortcomings show the areas that modern approaches are overcoming to achieve more effective C2 systems.

B. Hypernetworks and Supernetworks

Hypernetworks and supernetworks are alternative and complementary models to traditional graphs in the organization and management of network structures.

Hypernetworks are neural networks that generate weights for another neural target network and are useful in describing C2 networks with complex interweaving connections and dynamic topology. They represent an extension of standard networks in which nodes (or vertices) can be connected not only by single edges, but also by multiple edges, which allows for more complex interactions and structures. Hypernetworks offer multi-level interoperability, allowing integration and information exchange between them, and are often used to integrate data and services from different platforms and other sources [5].

Supernetworks are Internet Protocol (IP) networks that consolidate multiple smaller networks into a larger one, simplifying routing and reducing their size. They are typically more structured and organized than hypernetworks and can include existing networks working together to achieve common goals. They are often used to optimize resources, manage traffic, and improve the efficiency of network operations [6].

The main difference between hypernetworks and supernetworks is their structure and functionality. Hypernetworks are more flexible and integrate different networks, while supernetworks are more structured and pool network resources for optimization and efficiency.

A comparison of hypernetworks and supernetworks with traditional graph models outlines the following advantages of the former for C2 systems. Hypernetworks and supernetworks offer opportunities for decentralized management, flexibility, and adaptability in response to changing conditions or new requirements, which is essential for the speed of response in a combat environment. They are characterized by increased reliability, security, and protection of communications through duplication of connections and resources or through complex protocols and security mechanisms that increase the invulnerability of the network in the context of military and strategic operations. Hypernetworks and supernetworks have significant advantages in terms of data processing capabilities – they allow for parallel processing of multiple data, processing of complex data and information in real time, and working with large volumes of data and information, which is essential for the speed and quality of operational and strategic decision-making. They can integrate different technologies and platforms, which allows for flexible communication and coordination between different units of the system. Through effective resource management, hypernetworks and supernetworks can minimize losses and maximize the performance of C2 systems. Overall, they offer greater adaptability and connectivity between different networks and systems, while traditional networks are characterized by a stricter hierarchy and centralized management. Hypernetworks and supernetworks are extremely useful for C2 systems when they have to function in complex and dynamic environments or to improve security and coordination in complex situations.

II. MATERIALS AND METHODS

The method used is a comparative analysis of some of the latest scientific research in the field of hypernetworks and supernetworks development in the C2 systems. The main emphasis is on identifying the conceptual aspects of the models, although the technical parameters tested in the simulations are also noted, which generate conclusions about the effectiveness of the proposed solutions. The mathematical formulas with which the models are described are not presented in this report. The aim is to reach a wider audience through theoretical extraction. The cited studies were carried out by a team from the Chinese scientific academy in the field. At the same time, the models under consideration, in addition to being unique in their adopted research approach, also have a mutually complementary theoretical value. All authors in their conceptualizations proceed from the OODA (observe, orient, decide, act) ring theory of a C2 network, according to which combat process mainly includes three basic activities: battlefield situational awareness, decision command formulation, and firepower strike implementation. References to the C2 networks of the C2 systems in the Bulgarian Armed Forces are provided.

III. RESULTS AND DISCUSSION

A. Models of C2 Hypernetworks and C2 Supernetworks

The unprecedented increase in battlefield mobility, the expansion of the theater of operations, and the complexity of command and coordination relationships place higher demands on the functional characteristics of C2 networks [7]. The requirements for the inclusion of heterogeneous nodes, multiple connections, and time-varying topology complicate the traditional network model and form an avenue for the introduction of new advanced alternatives.

This report will analyse and compare several models of C2 hypernetworks and supernetworks, whose a priori assumptions are built on an identical pattern of structural simplification of the combat process based on the main functions and responsibilities that combat units perform - battlefield situational awareness, formulation of a command for a decision to act, and the execution of a firepower strike “Fig. 1”.

The three processes are represented in C2 hypernetworks and C2 supernetworks through three types of nodes - sensor, command, and combat. Each of these units forms its own unique subnetworks, which intertwine with each other to form a topological structure with multiple overlapping horizontal and vertical layers. The core of the network is the command subnet, which forms two interlayer networks with the sensor and firepower

nodes. The result is a three-layer, five-network cross-over structure "Fig. 2".

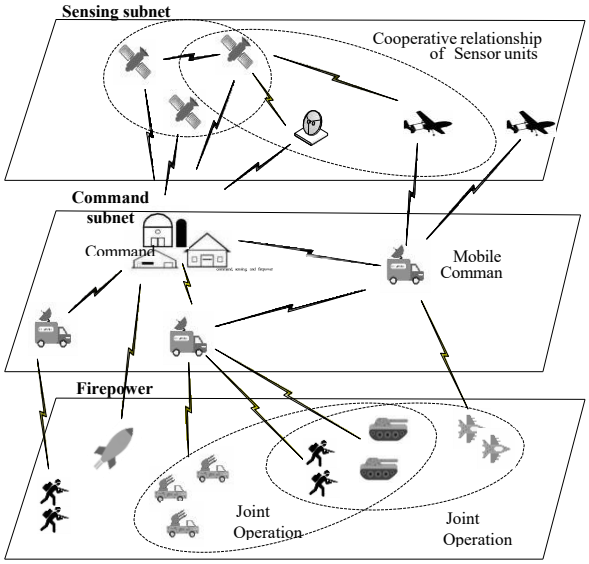


Fig.1 Example of a modern C2 network [10].

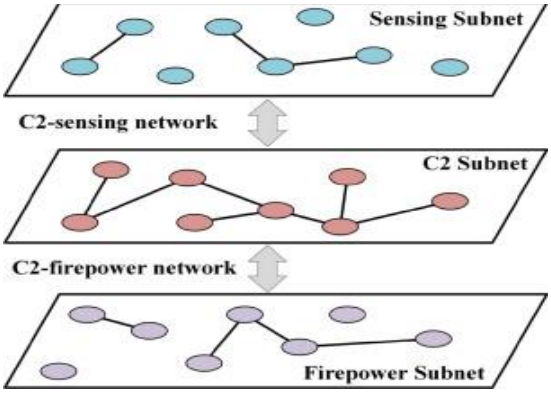


Fig.2 Abstract visualization of a C2 network [9].

The paper will present three models for C2 hypernetworks and C2 supernetworks, which, based on the simplified pattern of the combat process and applying unique algorithms, offer further conceptualizations of certain aspects of the behaviour and management of evolutionary C2 hypernetworks or C2 supernetworks. Wang et al. (2019) [8] propose an algorithm for hierarchical transformation of the layers of an evolutionary C2 hypernetwork model. Chen et al. (2023) [9] define rules for the evolution of different types of nodes and edges and propose steps for the dynamic development of a C2 hypernetwork. Chen et al. (2019) [10] propose a model for a C2 supernetwork based on the priority of the synergy of attributes, and analyse the rules for the evolution of the network hyperedge. The evolutionary aspect of the models means that networks are not static, but develop and change over time, which may include adding or removing nodes, changing the connections between them, and adapting to new conditions or external influences. At the same time, in order to reflect real-world performance, the authors adopt a number of constraints on the evolutionary behaviour of the structure and capabilities of C2 hypernetworks and C2 supernetworks. The first constraint is on the type of connected edge. It is assumed that the transmission of information between a sensor node and a firepower node must go through a command node, and thus the direct connection between a sensor node and a firepower node is not considered in the evolutionary process. The second constraint is on the uniqueness of a command link. In order to guarantee the uniqueness of a given command, sensor and fire strike nodes can only be directly connected to one C2 node. The third constraint is to combat the link integrity constraint. Only a complete combat link can be formed for combat effectiveness, which means that in the event of an attack, operations such as the removal and restructuring of isolated nodes must be carried out.

The following sections will present the main parameters of the models. The comparison of individual variations is carried out in order to identify the areas of application and the tasks being solved.

a) Hierarchical Evolutionary Model of C2 Hypernetwork

Based on the presented three-layer pattern, Wang et al. (2019) [8] build a model that uses the characteristics of nodes and their interactions as basic concepts. Each node has an identification number, uniqueness, attributes (the set of node functions, which is a vector), performance (the ability of the node to process data, perform calculations and communicate with other nodes). The information interaction between the types of nodes in the hypernetwork forms sets of hyperedges, described by a mathematical equation. An edge of the graph that contains several (arbitrary number) nodes is defined as a hypergraph. The interaction between different types of nodes is shown in "Fig. 3".

The figure illustrates the three layers of nodes, which can be grouped both within a given layer and in a hyperedge with nodes from another layer. In the general case, command nodes receive information from multiple sensor nodes and are connected to them via a hyperedge. Information exchange is possible between multiple command nodes, which is visualized by hyperedges between them.

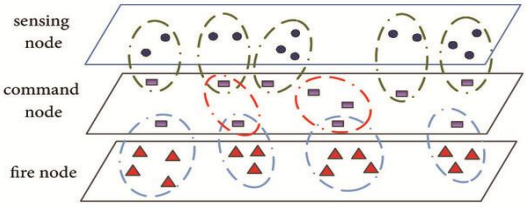


Fig.3 Wang et al.'s (2019) hypernet model for command and control [8].

One command node is authorized to command multiple fire nodes to carry out a fire attack against combat targets. A command node and multiple fire nodes are connected via

a hyperedge to indicate the downward connection to the fire attack command. Thus, the C2 hypernetwork model based on a hypergraph is able to relatively adequately describe and represent the interaction and influence between nodes.

The C2 hypernetwork model is represented by mathematical equations [8]. The applied conceptual approach includes a hierarchical modelling method that combines the hierarchical characteristics of the C2 network and the characteristics of the multilayer structure of the hypernetwork through the formula K(Mn + 1), where K is the total number of layers of the C2 network to be built, and Mn is the number of new nodes added in layer n. The model also analyses the frequency of node joining in each layer. The principle of operation of the hierarchical evolutionary model includes three steps: initialization (the hyperedge connects the nodes), increasing the number of network nodes (new nodes are connected to new nodes in a hyperedge according to probability) and hierarchical transformation (when the number of nodes increases in a given layer, a new layer begins to be built). The hierarchical process of evolution of the C2 hypernetwork deployed according to the defined steps is visualized in "Fig. 4".

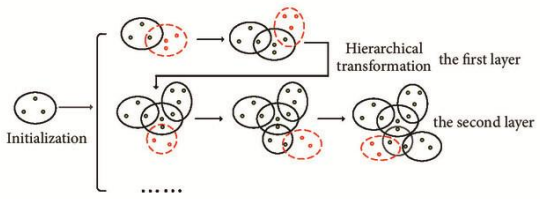


Fig.4 Diagram of the hierarchical evolutionary process of the C2 hypernetwork [8].

Theoretical analysis of evolutionary algorithms provides evidence that the degree of nodes in the C2 hypernetwork follows a hyperdegree distribution and has scale-free characteristics.

The model is verified by simulation, which shows that the characteristics of the C2 network "the rich are richer" are satisfied, i.e., a node in the network that already possesses many links or resources is more likely to attract even more links or resources.

In order to analyse the characteristics of the hierarchical evolutionary model of a C2 network, the changes of measurement indices such as average degree, clustering coefficient and modularity degree are simulated and analysed. The results show that the values of all three coefficients are significantly higher than those of other networks.

The simulation examines the invulnerability of the C2 hypernetwork to targeted or random attacks. The metric used is the natural connectivity coefficient. The results show that when the hypernetwork encounters targeted or random attacks, the natural connectivity of the hierarchical hypernetwork is higher than that of other networks with an increasing number of attacks, and the numerical value changes slowly. This means that the invulnerability of the hierarchical hypernetwork model is better than that of other network models.

In conclusion, although it is built on the hypothesis of simplifying information warfare, the hierarchical evolutionary model offers a framework that improves the efficiency of the C2 network, operates with heterogeneous nodes, multiple connections and different layers, offers better connectivity between nodes and greater reliability of the organizational structure. The model has an important reference value for building a C2 network topology [8].

b) Dynamic Evolutionary Model of C2 Hypernetwork

The evolution of the C2 hypernetwork refers to the process of dynamically adjusting the network structure in accordance with the combat process and the switching of combat missions to achieve coordination and cooperation between subnetworks. Chen et al. (2023) [9] proposed a method for dynamic evolution of the C2 hypernetwork, in which the dynamics of behaviour are categorized as the addition and deletion of combat units (nodes) and the establishment and dissolution of combat relationships (edges). The characteristics of the dynamic evolution of the C2 hypernetwork are the heterogeneity of nodes and edges; dynamic changes of nodes and edges; synergy between homogeneous nodes. The interactive relationship between nodes of the C2 network is expressed in a network model with dynamic characteristics of edge connection.

Behaviour addition. One way to improve the combat capabilities and efficiency of network transmission is to add new combat units (nodes) and establish new connections (edges) in response to updated operational requirements. Three categories of node additions have been described, which are described by mathematical formulas (see Chen et al., 2023). The main theoretical considerations for each process are as follows:

- Adding a C2 node. The probability of joining a C2 node decreases as the command hierarchy increases. If the added C2 node joins the highest command hierarchy, a cooperation boundary is established with all C2 nodes in the hierarchy.
- Adding firepower nodes. The purpose of adding a firepower node is to improve the combat capabilities of the C2 network or to compensate for the lack of current combat capabilities. The attributes of a firepower node typically include mobility, fire suppression, and air defence capabilities.
- Adding sensor nodes. The addition of sensor nodes is done to increase the type or extend the range of intelligence, thereby improving the network's understanding of the battlefield situation, allowing C2 nodes to make more accurate command decisions.

In parallel with the addition of nodes, new joint connected edges can be added. The act helps to improve the ability to share information and carry out joint commands. Three rules are defined for adding edges: for cooperation with a C2 node; for cooperation with firepower nodes; joint edges to a sensor node.

Deletion behaviour. In the C2 hypernetwork development model, node deletion is considered within two main scenarios: normal node elimination and as a result of enemy fire.

- Normal node elimination. Deletion of poorly connected or non-working nodes.
- Elimination of nodes during enemy attacks (random or intentional attacks).
- Active deletion of connected edges. The hyperdegree values of the nodes at both ends of the connected edge are used to measure the importance of the edge. Nodes with low attributes or those that have acquired them during resource consolidation are likely to be actively deleted.

Behavioural Restructuring. In the process of C2 network evolution, isolated newly created nodes may be added to the positions of deleted nodes. In these cases, these isolated nodes need to be reorganized to improve the invulnerability of the C2 network. Common reorganization methods include level-up, cross-level, transfer, and upgrade. Due to the strict hierarchy of the C2 network and the synergy between nodes in the same command hierarchy, the authors only consider the node transfer method.

- Transfer and Reorganization of C2 Node. When a C2 node in a certain command hierarchy is deleted, the subordinate node directly connected to it loses its command relationship, and then needs to be reorganized.

Simulation analyses show that the proposed model has the characteristics of a scale-free network and obeys the law of hyperdegree distribution. Parameter analysis shows that in the network construction stage, the evolutionary behaviour is mainly manifested by the increase of nodes and edges. At the same time, node deletions also occur due to normal elimination. The results show that the increase in the number of new nodes increases the size of the network, and the characteristics of network scarcity also gradually appear. At the same time, the average length of the information transmission path between nodes increases and the average clustering coefficient of the network decreases. In addition, the increase in edges optimizes the organization of the internal connections of the network, improves the information interaction ability and the proximity between nodes, thereby shortening the average length of the network path and increasing the average clustering coefficient of the network. Due to the fact that the number of steps in the network development increases, the average path length of the network shows a decreasing trend.

The analysis of the network invulnerability is carried out in the confrontation stage, when the C2 network is subject to external attacks. In this situation, the behaviour of the network evolution is mainly dictated by the probability of removing nodes and edges. For two typical attacks, random and intentional attacks, the removal methods can be classified as random and preferential with hyperdegree. Under random attacks, the network performance decreases slowly. The reason is that random attacks have the same probability of removal for each node, and the C2 network has an approximate tree structure and an interlayer cooperative structure, which allows compensation mostly by cooperative edges. Intentional attacks are aimed at critical nodes and the clustering coefficient and the combat effectiveness decrease significantly more than random attacks. The simulation shows that the relatively highest invulnerability shows a network in which the hyperdegree is only one of the considered factors and takes into account the reorganization behaviour of isolated nodes [9].

In summary, the results of the simulation analysis show that the dynamic evolutionary model of the C2 hypernetwork is able to maintain relatively good network performance under both random and intentional attacks.

c) Multilevel C2 Supernetwork Model Based on Attribute Synergy Prioritization

Chen et al. (2019) [10] propose a multilevel C2 supernetwork (MC2S) model based on attribute synergy prioritization. The approach adopted takes into account the differences between inter-layer and intra-layer hyperedge generation, as well as the differences between nodes of the same class that have different attributes.

In addition, strategies for generating intra-layer hyperedges in the MC2S model based on attribute synergy prioritization, as well as methods based on a local world (LW) model for generating inter-layer hyperedges of the network, are described.

The MC2S model is based on the described three-layer pattern consisting of command, sensor, and fire subnetworks. Within the model, the cross-layer structure of three layers and five networks is considered as a supernetwork or “network of networks”.

In the sensor layer, the node attributes are defined as communication information collection capability, image information collection capability, and intelligence data collection capability.

Firepower nodes have four operational capability attributes, namely, advance capability, firepower neutralization capability, air defence capability, and equipment maintenance capability.

The core of the network is the command subnet, which forms (two) interlayer networks with the sensor and firepower level nodes. The command scope and command level of the network are with command levels that are consistent with the organizational structure of the Army C2 systems.

Attribute synergy prioritization is applied as a comprehensive boundary generation strategy to determine the attraction between nodes and the connection between them. The rules for intra- and inter-layer hyperedge generation are based on attribute complementarity. In intra-layer networks, cooperative intra-layer hyperedges are formed between firepower and sensor nodes based on their attraction to each other (as determined by the attribute

synergy rules) to provide a wide range of operational capabilities required by a combat mission. In inter-layer networks, inter-layer C2 links with LW selection characteristics are formed between command nodes and firepower/sensor nodes based on their hyperedges. This process ensures the efficiency of information transfer between nodes of the intra-layer cooperative hyperedges. In summary, attribute synergy prioritization forms the basis of the proposed model.

Simulation results show that possessing small-world properties provides high levels of information transmission efficiency between combat units of a C2 network. The MC2S model has a short average path length as well as a large clustering coefficient. In general, low average path lengths allow combat intelligence to quickly reach a target node, while large clustering coefficients indicate that nodes are closely connected to each other, which increases the efficiency of command issuance and joint combat.

The hyperdegree distribution of the model approximately adheres to a power-law distribution and therefore exhibits scale-free properties. Most of the sensor and fire nodes possess very low hyperdegrees, indicating that these nodes will perform their missions independently in most circumstances. However, the distribution is distorted at high hyperdegrees and in these cases deviates from the power law.

Nodes with significantly high hyperdegrees (such as reconnaissance satellites) can participate in different missions through cooperative relationships. The class-specific hyperdegree distribution of command nodes is that there are high connection probabilities at low hyperdegree and low probabilities at high hyperdegree, which indicates that the C2 network possesses the characteristics of centralized command. In addition, the hyperdegree distribution of command nodes shows a significant “lift”, and most of the command nodes around the peak of the lift are third-level nodes, which indicates that the base-level command nodes need to be connected to a large number of sensor and fire nodes to direct battles and obtain real-time information for battle. Thus, this structure helps to divide the workload of high-level command nodes and improve the efficiency of combat command.

The next parameter to be analysed is the efficiency of the network superlinks. It is assumed that the mission link in a supernetwork is defined as the shortest chain of hyperedges between layers between sensor nodes and firepower nodes. Generally, the focus of network evaluations in the real world is the overall combat capability of the network.

This metric can be expressed using the total number of missions superlinks in a network and the average efficiency of these mission superlinks.

The dependence of the overall network combat capability on the tuning parameter of the joint propensity of the surveillance and firepower subnetworks indicates that increasing the number of interacting edges will effectively increase the network combat capability.

The author team considers the cost of network construction as an important factor to be considered when developing C2 networks. The test results show that it is cheaper to increase the network combat capability by improving the level of cooperation in sensor nodes than by improving the level of cooperation in firepower nodes. Therefore, it is important to increase the level of interconnection in the sensor subnetwork during the construction of C2 networks in the real world. Since the construction of C2 networks is a multi-attribute decision-making problem that is constrained by various factors, the authors emphasize the need to holistically consider mission difficulty, network cost, and network performance during the configuration of C2 network parameters.

In any mission that requires a specific set of node classes, the combined cooperative combat length of this set is the sum of the shortest path lengths between any two nodes divided by the maximum number of links between the nodes of this set. Since C2 networks are intended for use in combat missions, the efficiency of communication between nodes participating in a mission is an important indicator for determining the cooperative engagement capability of a C2 network. The authors propose the combined cooperative combat length as an indicator of this capability in supernetwork models that contain nodes with different classes and attributes.

The information transmission efficiency of the considered model is proven to be significantly higher than that of other models and is most pronounced in simple missions. Thus, the characteristics of the MC2S model are suitable for forming effective and stable cooperative structures in nodes with different attributes during the execution of certain combat missions. In this way, the combat capability of the network is proven to be greater than that of individual nodes [10].

Network invulnerability indicates the ability of a C2 network to maintain connectivity when attacked. In all C2 network models, the network performance decreases slowly in the presence of random attacks; however, it degrades rapidly when subjected to selective attacks. Thus, these C2 network models are robust against random attacks but weak against selective attacks. Since these network models have significant preferential attachment properties, there are a small number of nodes that play a central role in these networks, and the removal of these nodes through selective attacks can have a significant impact on the C2 network. Nevertheless, the MC2S model maintains the highest overall level of combat capability in both scenarios and shows an excellent degree of invulnerability.

Appropriately adding connections between nodes in the firepower layer or sensor nodes in a C2 network will help prevent key nodes from being isolated when the network has suffered a failure, ensuring that the network's mission connections remain intact during combat, thereby improving the network's ability to sustain combat.

In conclusion, the simulation experiment results prove that the proposed MC2S model possesses small-world properties, scale-free properties of supernetworks, and high level of network robustness. In addition, the hyperedge

connection based on attribute synergy prioritization in the model significantly improves the cooperative engagement capability of the network. In summary, the model is a reference for describing heterogeneous edge connections in C2 networks, analysing network performance, and deploying complex networks for combat missions in the context of the integrated joint operations doctrine [10].

D. Application of Hypernetworks and Supernetworks in the Context of C2 Networks of the Bulgarian Armed Forces

The communication and information characteristics of the military CIS networks are a matter of secret nature and, according to some experts, the general system does not include hypernetworks and supernetworks. The defining concept is Integrated CIS [11], [12], [13], [14]. Regardless of the fact, supernetworks can be indirectly established as applicable components in the system architecture. Supernetworks, also known as Classless Inter-Domain Routing (CIDR) and the process of combining multiple networks into a larger network, allows for more efficient use of the IP address space, leads to improved scalability and reduced network load. "Classless routing" between domains (Classless InterDomein Routing - CIDR) is widely implemented in the Bulgarian Integrated CIS [15].

An example of the presence of a supernetwork includes the infrastructure of one of the latest purchased digital communication and information means for the Land Forces of the Bulgarian Army for equipping a brigade and battalion command post [16]. The new equipment allows for the transmission of voice, data and video in real time from a camera mounted on the helmet of the foot soldier to the battalion commander and to higher levels, depending on the mission. The acquired information system for command and control provides services at three levels: foot soldier - combat vehicle - command post. The system supports the operational staff in joint planning and execution of missions, building a generalized picture of the ground situation and enabling commanders at different levels of command to make the right decisions and promptly give their orders to the last soldier "Fig. 5".

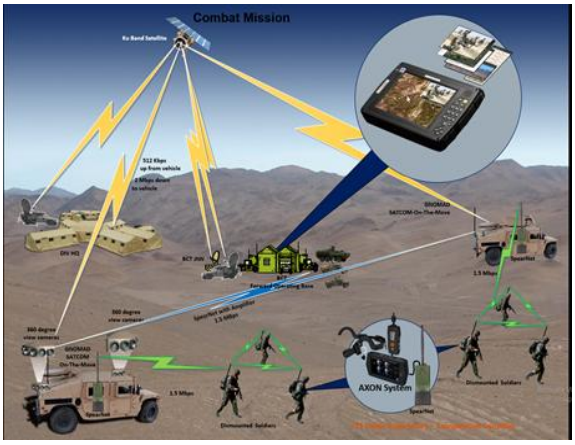


Fig. 5. Supernetwork model "foot soldier – combat vehicle – command post"

In addition, part of the new equipment are radio relay radios, providing stable broadband communications with a transmission speed of up to 428 Mbps, through which the necessary services are provided to the control points. The installation of dual-channel VHF radios, which allow simultaneous voice communication and data transmission at speeds of up to 5 Mbps, has a software-defined architecture and supports rapid updates in the field. Routing and cross-connect capabilities ensure the sharing of critical ISR for voice and data with different networks and subnetworks. The "foot soldier – combat vehicle – command post" model is an alternative version of the "sensor layer – command and control system – fire layer" model, which was considered in the theory review.

A problem with national defence capabilities is that the systems in place "provide services – voice, data and video, but they are built on the basis of different technologies and the compatibility between them is highly limited, and in some cases even impossible" [17, p. 127]. It is recommended to "generate a strategy for building the communication and information system, through a technologically derived concept for rearmament and with capabilities for an adequate response to hybrid threats" [17, p. 130]. In such a context, the application of hypernetworks and supernetworks gains its place.

CONCLUSIONS

Hypernetworks and supernetworks offer compensatory mechanisms to overcome some limitations of traditional graph theory when applied to C2 networks. The comparison of the individual variations of the conceptual approaches was carried out with the aim of identifying the areas of application and tasks to be solved. Each of the described models offers a specific contribution to improving aspects of the functioning of a C2 network in combat conditions. The hierarchical evolutionary model of Wang et al. (2019) presents the algorithm for implementing a hierarchical transformation of a C2 hypernetworks. Chen et al. (2023) illustrates the rules for dynamically changing the behaviour of an evolutionary C2 hypernetworks by describing the steps of removing, adding and reorganizing nodes and edges in the network. Chen et al. (2017) deploys a multi-level model of a C2 supernetworks by prioritizing the synergy of attributes. The three models are based on an identical three-layer pattern of the combat process and represent scale-free networks that obey a hyper-level distribution. All three models demonstrate good performance in terms of network invulnerability. Specific practical implications for C2 systems are the following:

- The performance of the C2 network is higher when optimizing the cooperation of sensor nodes than by adding fire nodes.
- The resilience of the C2 network is much higher under random attacks than under directed attacks. The destruction of key nodes can be compensated by adding additional connections between nodes in the firepower layer or sensor nodes.

- Increasing the number of growing edges will effectively increase the combat capability of the whole network.
- The cost is lower if the combat capability of the network is increased by improving the level of cooperation in sensor nodes rather than by improving the level of cooperation in firepower nodes.

In the Armed Forces of Bulgaria, the concepts of hypernetworks and supernetworks are not yet popular enough in everyday use, although in the case of supernetworks, they are recognized as woven into the name of older, classically established terms. The progressive process of modernization of the Bulgarian Army and Armed Forces and the introduction of new technologies in the form of newly purchased equipment puts both types of networks in the focus of attention. This report represents a step in getting acquainted with the conceptualization of the concepts and their widespread use for educational and scientific purposes.

ACKNOWLEDGEMENTS:

The document was developed under the National Scientific Programme "Security and Defence", funded by the Ministry of Education and Science of the Republic of Bulgaria in implementation of the National Strategy for the Development of Scientific Research 2017-2030, adopted by Decision of the Council of Ministers No. 731 of 21 October 2021.

REFERENCES

[1] T. J. Richard, Introduction to graph theory. New York : Dover Pub, 1993, pp. 8-18.

[2] E. Enev, "Understanding the operational environment and determining the center of gravity through network analysis and social network analysis," Bulgarian Science, vol. 05, pp. 8-16, 2020.

[3] M. Révay and M. Líška, "OODA loop in command & control systems," Communication and Information. Technologies, Vysoke Tatry, Slovakia, pp. 1-4, Oct. 2017.

[4] X. Song, S. Y. Zhang and X. C. Shi, "Measurement of network complexity and capability in command and control system," Journal of Statistical Computation and Simulation, vol. 84, no 6, pp. 1232-1248, Jun. 2014.

[5] V. K. Chauhan, J. Zhou, P. Lu, S. Molaei, and D. A. Clifton, "A Brief Review of Hypernetworks in Deep Learning." Artificial Intelligence Review, vol. 57, no 9, pp. 250-279, Aug. 2024. https://doi.org/10.1007/s10462-024-10862-8.

[6] A. Nagurney and T. Wakolbinger, "Supernetworks: An Introduction to the Concept and its Applications with a Specific Focus on Knowledge Supernetworks," The International Journal of Knowledge Culture and Change Management Annual Review vol. 4, no. 1, pp. 1-16, Jan. 2005. https://doi:10.18848/1447-9524/CGP/v04/50227.

[7] C. Pan, X. Chen, Y. Wang and B. Chen, "A method of key links identification in command and control network based on bridging coefficient," in IEEE ICNSC, Zhuhai, China, pp. 1-5, Mar. 2018.

[8] Y. Wang, B. Chen, X. Chen, and C. Pan, "Hierarchical Evolution Model of Command and Control Network Based on Hypernetwork," Hindawi. Journal of Control Science and Engineering, vol. 2019, no. 1, Jan. 2019. https://doi.org/10.1155/2019/5860461.

[9] B. Chen, H. Tao, X. Jiang, Y. Chen, and X. Gao, "Dynamic hypernetwork-based evolutionary model of command-and-control network," Simulation Modeling Practice and Theory, vol. 126, 102759, pp. 1-13, Jul. 2023. https://doi.org/10.1016/j.simpat.2023.102759.

[10] B. Chen, H. Yu, Y. Wang, X. Gao and Y. Xu. "Multilevel Command and Control Supernetwork Modeling Based on Attribute Synergy Prioritization," IEEE Access PP(99):1-1, Mar. 2019. https://doi:10.1109/ACCESS.2019.2903520. [Accessed January 25, 2025].

[11] K. Dimitrov, Planning and Design of Military Communication and Information Networks and Systems: Military Academy "G. St. Rakovski" Press, 2021.

[12] K. Kalchev, "Structure of a Military Communication and Information System Providing Network Connectivity," CIO Chief Information Officer, no. 7, 2010.

[13] I. Hristozov and M. Lambeva, Approach to Integration of Information Systems: Scientific Conference: Military Technologies and Systems for Ensuring Defense, Institute of Defense, Sofia, Bulgaria pp.176-182, 2012.

[14] I. Hristozov, V. Alexandrova, I. Chakarov, Ch. Kostadinov, K. Krumova and R. Angelov, Tools for Modeling Threats and Cyber Intelligence Processes Used in NATO, and Their Applicability: Collection of Reports from the International Scientific Conference: 20 Years of Bulgaria in NATO and NATO in Bulgaria. April 2–4 2024, Military Academy "G. S. Rakovski", Sofia, p. 235-246, 2024.

[15] Hristozov and Kr. Krumova, Computer Networks and Communications, Sofia: Military Academy "G. S. Rakovski", 2023.

[16] D. Mitev, "Digital transformation will cover all formations of the Armed Forces," Bulgarian Army Newspaper, Interviews, December 2023, [Online]. Available: https://armymedia.bg/2023/12/08 [Accessed January 27, 2025].

[17] I. Chakarov, National Defense Capabilities in Integration of Electronic Communication Networks: 30 Years of the Faculty of National Security and Defense 1994 – 2024 Anniversary Scientific Conference November 4, 2024, Military Academy "G. S. Rakovski", Sofia, pp. 123-132, 2024.

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025 Volume V, 119-126

The Role of Insects and Worms as Agents of Bioterrorism in the Atmosphere of Post- 9/11 America

Mirosław Grewiński
Departament of Social Sciences
Korczak University - Academy of Applied Sciences in Warsaw
Warsaw, Poland
mgrewinski@gmail.com

Marek Kawa
Departament of Social Sciences
Korczak University - Academy of Applied Sciences in Warsaw, Poland
m.kawa@uczelniakorczaka.pl

***Abstract*—The paper examines an importance of symbolism of microcosm engaged even into the bioterrorism rethoric used in the past September 11 (2001) media language in American public and politics and also on present public narration. The object of our review and study is a more constructive, cultural image of a bug (also 'electronic bug'), worm or insect as an element of various discourses in American media culture after terrorist 9/11 attacks in 2001. Since those events the approach to microcosm was stimulated in USA by the imagination of fears derived from the parthenogenesis, mass, parasitism, amorphous structures, destructive decays...etc. These figures of meaning are primarily attached to mostly pejorative content. The instrumental use of micrology for military and terrorist purposes today is a matter of common knowledge. Direct bio-attacks in that period of 2001-2002 were indirectly treated as a threat to the freedom of information exchange, and on the other, as a disturbing attempt to anticipate possible counterattack from the side of the U.S. Viruses, germs, bacteria or other pathogens, as semiotic and symbolic prolongation of the threat of "foreigners", especially terrorist forces. The main method of research which is involved within the article is desk research and review of American popular media – both paper and elctronic forms.**

Keywords*— *bioterrorism, worm, electronic bug, viruses, microcosm, American media, 9/11 attacks in New York City.

I. Introduction

In the presented approach the taxonomic definition of vermin, worms, insects, germs as the objects of cognition and research from the zoological-scientistic point of view is the secondary context, for the authors much more important is an analysis of all such small and the smallest phenomena from the postmodern social and cultural point of view. Although this paper treats "microcosm" in more general way, it is not binding, and consistent with the current state of the zoological art knowledge, findings on species classified as vermin. Zoology here appears only as one of the possible, providing specific images and meanings, discourse. But a simpler discourse of common people who on daily basis do not deal with special explications and used to refer to microcosm just occasionally is also important for our short diagnosis. Object of our cognition and study is a more constructive, cultural image of the worm on the level of literary criteria: as a lexem, symbol, image, motif, archetype, element of the *topos* (gr.), aesthetic-poetic convention, rather than its zoological equivalent – worm or insect *sensu stricto*. It reminds us slightly the situation of the worm in Hebrew, where its name was meant in *sensu largo* and was referring to all small crawling creatures on earth. The Bible also generally used formally two words to describe a worm: *rimmâh* or from Latin - *vermiculus*, especially since the worm belongs to a quite symbolic biblical (also religious) zoology which hardly can be missed in a comparative analysis. We may find out similarly that commonly called worms can be freely identified as worms sensu stricto (eg worms, worms, tapeworms, leeches), as well as any invertebrates, insects, larvae of insects. [1]. Worm or bug as a element of various discourses in European and American culture turns out to be a figure, motif, symbol, allegory...etc. These figures of meaning are primarily attached to mostly pejorative meaning. Hence we will try to make a brief cross-sectional review of their "occurrence" in imagination of Americans and politicians specially in so called post 9/11 time on the examples of enunciations of American media. There will be also some traits of American pop culture mixed with tradition of political-ideological propaganda.

The state of being a "small" or even "micro", to which worms, insects are belonged to, in the past as well as in

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8495
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

modern times was generating the less or more justified images, symbols, metaphors, and connotations. Mostly worms have been treated as all sorts of subject of suspicion, distrust and unequivocally negative imaginative projections [2]. It does not mean that in these days people are not afraid of any new micro-creatures (see casus of anthrax, HIV virus, SAARS, Ziko, disturbing bacteria Escherichia coli, coronavirus COVID-19 ... etc.) as microcosmos reveals itself outside. And the reasons and opportunities for this ambivalent attitude of the former mentality to the microfauna sphere have not changed yet too much. All microorganisms which stimulated the imagination have become also another source of fears, threats and provided useful images which we can take into account here for our comparative analysis. Some features related to cultural perception of vermin creatures can be raised sometimes in characterizing such phenomena as mass culture, massive objects or aliens. These vermin-analogy characteristics include for instance parthenogenesis, masses, parasitism, amorphous structures, destructive decays...etc. To some extent words of Dwight Macdonald refer to this mentioned parallel talking about the essence of popular or mass culture: „It is true that mass culture was born - and to a certain extent it is still today - as parasitic, cancerous growth (ulcer) on a higher culture. [...] However, there is no type of relationship like between the leaf and the branch, but rather it imitates the relation between a caterpillar and a leaf. Mass culture undermines the higher culture as if were situation of unpredictable settlers who extract wealth from the land [3].

From the point of view of history it has to be remembered that the most tragic for the Jewish people were associations and comparisons, exploited by racist Nazism in Germany, comparing them to parasites and vermin in relation to social affairs and referring to the role of Jews in trade or usury, especially when Hitler came to real power in 1933. Due to propaganda efforts, especially in the context of developing audiovisual media, Hitler succeeded on an unprecedented scale to create the image of a Jew-parasite and to install it in the mentality of most Nazi Germans [4]. Declared reluctance towards the Jews was more than once expressed by means of the generically meaningful motif of the vermin as the main imagery attribute that is identified with this ethnic-religious factors. These symbolic offensive attacks - as it turned out - were formulated at various times, for various reasons and by various characters. The authors of such racial depictions and caricatures sometimes made by very noble and respected persons because of its place in literature or culture and others were simply anti-Semites [5]. A quite known sociologist - Zygmunt Baumann tries to explain Hitler's tendency to comitting attrocities and crimes through his interpretation of Hitler's keeping hygiene and clean what he was revealing from the very begining of his life of political activist. Therefore Hitler's altitude to Jews, Gypsies, the disabled, sick, and other victims of Nazi German genocide can be interpret by means of traditional archetype and opposition "clean - unclean". But not only the Jews were the victims of propaganda suggesting to enemies of being as worms or antiseptic allusions. Here, though still in the German propaganda of the prehistoric times in Germany and Nazi triumph of German propaganda engaged this suggestive image towards German's enemies. For example compiled propaganda materials from the struggle for Upper Silesia in the time of the March 1921 plebiscite in German they have been mocking the alliance of Poland and France during the dividing of Upper Silesia: "In the drawing entitled« French Purity » there is shown sitting in a chair in a German room with the will of a treaty a French officer with insects symbolizing Polish soldiers crawling over the floor in the corners, walls and even on the French officer's leg..... " [6]. Also, several years later then, Soviet propaganda will be exploiting in its discourse a caricature picture of an insect imitating a Polish general pierced with a knife as a reaction to the defeat of Poland in September 1939 year [7]. From the cultural and historical perspectives the worm was seen as a tangible sign of the interference from deities, the sacred, the aliens, usually seen mostly as an envoy from the sphere of the infernal entropy to bring the same process down on earth. Therefore worms stood in the eyes of people as a cruel tool for revenge and punishment; moreover the demonic worms among others "causes" like heretics, witches, doctors, dissidents, Jews, Gypsies, Jesuits, etc. have been blamed for deliberate infection or indirect providing deadly epidemic plagues; these mechanisms of social psychology exploiting the image of worms as a danger from nowhere (microcosm) exist unfortunately also till now, but in different already contextual configurations adjusted to today's reality and mentality. The position of former demonic actors coming from micro-world which used to be worms has been replacing by new imaginative forms of fear like special services, ethnic minorities, sexual deviations, secret relationships and organizations ... etc. It can be proved though by an example of the colloquial and sometimes peculiar "popularizing" the works of various interpretations of contemporary AIDS epidemic relating on various arguments and their interpretations, here is a sample:

" The cause of AIDS is the abuse of using narcotic drugs; this God's penalty for homosexuality and prostitution; mutants, formed as a result of trials with nuclear weapons, they converted an harmless microbe into a deadly virus; as a result of malaria experiments there have been accidental virus infections of monkey by scientists and they spread the microorganism to others" [8].

Such fears and allegations towards microorganisms more or less logically justified we also found in political and social discourse after time of healing social and mental wounds of American society of 9/11 attacks in 2001. Moreover, post 9/11 period was undoubtedly political, economic and mentality change in American society and media, where the terrorist attack on September 11, 2001 in Manhattan of New York City became a specific turning point in American thinking and looking at reality. During that time, our research interests related to the cultural perception and presentation of the microcosm, which resulted in the following research, which also revealed a specific record of that "post-September" atmosphere of

danger and suspicion towards microorganisms as microbes, germs, bacteria, viruses, insects, worms…etc. without zoological taxonomy differentiations but for mostly regarded from the cultural points of view. As observers of those behaviours and American reactions to the bio-terroristic threats we decided to examine them with new interpretative contexts.

II. Materials and Methods

Authors of this review of mostly American press media from the period of the post 9/11 anxiety caused by the tries of bioterrorist attacks in years 2001-2002. Therefore, the main method of research which is involved within the paper is a desk research and review of some data and diaries of the authors who were travelling in USA in years 2001-2003. A small amount of contribution comes from the own experience of the authors who have watched American electronic media as well.

III. Results and Discussion

A. What were the typical examples of the bio-terroristic threats and reactions of American society?

More than eighty years ago, before the advent of radio and television, Walter Lippmann (1922) observed that what people know about the world around them is mostly the result of second- hand knowledge acquired by reading newspapers. In modern-day mass societies, people are even more dependent on the news;" [9]. The period of media narration, which we are trying to review shortly too, still belonged to postmodern and globalist time before the dominant outburst of social media which actually started more or less around 2007. Even when individuals witness events, such as a devastating terror attack or massive anti-war demonstrations, or when people are affected by socioeconomic developments, such as high unemployment or increasing energy costs, they are still likely to depend on the traditional source of news to explain the reasons, consequences, and political significance of what they have experienced personally. Both entertainment and news media have always paid extraordinary attention to violence regardless whether in the form of crimes or acts of terrorism. Especially in television network news and local news programs terrorism outpaced by far other important events, issues, and problems. It is worthy to indicate that between 1981 and 1986, more news stories were broadcasted (mentioning only three TV networks ABC, CBS, and NBC) on terrorism than on poverty, unemployment, racial inequality, and crime combined. Hijackings, hostage situations, and similar events. Major anti-American attacks took place inside the United States (the first World Trade Center bombing in 1993, the Oklahoma City bombing in 1995) and abroad (the Khobar Towers bombing in 1996, the bombings of the U.S. embassies in Kenya and Tanzania in 1998, the suicide attack on the USS Cole in 2000). But the most broadcasted „live" moments of terrorist attack ever probably took place just on 11 September of 2001, when hijacked planes hit the towers of WTC in New York City: traditional media as radio, networks provided all day and night coverage; at least two cable shopping channels and Chicago's WPWR-CH.50 ceased regular programming out of respect for events. Cable sports channels and even MTV and VH1 canceled regular programming to run coverage from their corporate-sibling news organizations. Authors of this paper were being in the U.S. that time and witnessed as several local stations used their relationships with other stations to air news coverage. Channel 50 showed CBS, WCIUCH.26 aired channel 9's CNN coverage; WCPX-CH.38 channel aired NBC news programming.

Nationally, all the networks, in a rare moment of cooperation, shared their live feed without credit or logos attached. Televising hijacked plane hitting north tower in NYC, and collapsing towers was reminding killing Lee Harvey Oswald by Jack Ruby in the eye of American public in 60's. Even worse not only crumbling towers but people diving out from the top floors of burning WTC towers. The 9/11 attack undermined the claim that the rich and powerful, sophisticated missile-defence system can shield such super geopolitical powers as USA.

On 13th September 2001, one of the daily popular columnist and commentator from „Chicago Tribune" John Kass wrote: "For the past decades we have sat dumb and stupid as the U.S. military was transformed from a killing machine into a playpen for sociologists and political schemers. [10]. The one of primary goals of terrorists was to intimidate their target publics and force governments to react and often over-react or to get an enemy paralyzed But government officials who are responding to terrorist attacks were also in excellent positions to utilize the media to enlist public support for their policies.

In post - 9/11 atmosphere the feeling of American security that the Capitol (the United States Congress's architectural complex) had been out of reach of the totalitarian regimes, terrorist attacks, internal and economic unrest, once again was undermined just after 9/11 quite fast but on October 18th of 2001. One of the cause was bacteria called *Bacillus Anthracis.* The range of possible germs is vast, but there are some mutated pathogens that are particularly capable of causing chaos. The NATO guide to potential biological weapons lists 31 infectious agents. The top five are such as anthrax, smallpox, plague, botulism, and tularemia. Anthrax has always been at the top of the list of diseases that cause real terror [11] . It may even have been a major factor in one of the first recorded cases of biologically assisted political persuasion—one of the first plagues to hit Egypt in the time of Moses. Even today, most experts still consider anthrax to be a very potent and effective weapon. This species of bacteria (*Bacillus Anthracis)* appears all over the world and regularly causes natural cases of the disease. American anthrax victims learned that these bacteria can be transmitted by inhaling them from the air or even scratching the skin. Eating raw meat can also have the same effect. The first symptoms begin to appear after 1-5 days. The skin infection kills 1 in 5 people, but when the bacteria get into the lungs, they kill almost every victim within 2 or 3 days. They produce a toxin that not only attacks our body but also disables our immune system, thus leaving us completely helpless in the

face of the attacker [11]. But this virtual to some extent anxiety was caused at that time also by the SAARS virus and the West Nile Virus which were affecting convenient American way of life much and deeply in some parts of States. For instance the West Nile Virus particularly touched the American continent. The authorities of Louisiana state reported 14 new cases of West Nile Virus (which caused two deaths). Authorities along with 20 scientists from the Centers for Disease Control and Prevention have admitted they are unable to stop the spread of the virus, which hit 85 people and killed 7 people. There were 128 cases nationwide. In 90 cases, 60% of the subjects in the lab might be positive, as doctor Raoult Ratford, the state epidemic inspector from the North Dakota State Department of Public Health, suggested. There was also no reduction or halting of the development of infections, and therefore more and more concerned people were trying to check their results, hence the frequency of visits and tests passing. It should be indicated that the Virus West Nile used to be transmitted mostly by migratory birds and spread by mosquitoes. Deadly specimen of such an infected bird were found, among others. In Baton Rouge in May (2002) [12]. Persons infected with this virus can manifest influenza-like symptoms as well as in some cases encephalitis or swelling of the brain. First discovered in the West Nile in Uganda in 1937, the virus has spread to Europe, Middle East Asia and North America. In summer of 1999 seven New Yorkers died during the first outbreak of the virus in the United States. Since then, the West Nile has killed 22 people in 34 states. The first cases appeared in New York in 1999, then at that time 55 people were hospitalized, seven were the fatalities. In August 2002 there were 128 human cases across the country. Those casualties of the virus sooner or later had to cause a sort of social fear. Despite this fear we should admit that terrorists, internal bio-attacks were not for the American society anything new. They had experienced at least the cases like the Oregon accident of September 1984 and 1985, when followers of the Rajneeshee sect spread Salmonella Typhimurim (what resulted in 751 cases of gastroenteritis and multiple hospitalizations). The investigation did not succeed and there was no sure whether the appearance of anthrax molecules was yet another attack of Al Qaeda or a maniacal incident.

For a cultural and psychological interpretation, the diagnosis of the mental consequences of a criminal offence is much more important. Referring to anthrax again it should be stressed that this bacteria caused more confusion in the House of Congress and American media than many other earlier political events. In spectacular cases of finding presumably pollen of anthrax in presence of such American as Robert Stevens from Florida (the official photographer of The Sun magazine) or New York - Ernesto Blanco (a NBC correspondent), New York Governor George Pataki, or the habitants of Washington at last (31 employees of Capitol) who had probably dealt with almost invisible pollen distributed by mails. Powdered spores of a single-celled bacterium (1-5 microns) were found in the office of Senator Tom Daschle, who was in that time important the Senate Majority Leader. Unfortunately, anthrax in its pure form of bacterium produces dangerous toxins, and possible infection can be occurred in three ways: skin infection through wound, pulmonary-inhalation and the rarest type - through the digestive tract when raw meat is ingested [13]. At the same time, it is worthy to underline a *sui generis* perfidious feature of the phenomena of microcosm: because this simple bacterium can exist only in tissue and blood, but over time, when the infected carrier dies, the bacterias are formed and transformed into spores - which imitate the structure similar to the semen and through the resistant immunity crust can survive for at least 100 years until the next host is found.

American society was concerned about the fact that a fairly probable, predictable, thoroughly researched and controlled bacterium (most of American universities and research centers were working on bacterial material, and 1,200 American laboratories in October of 2002 conducted current anthrax studies) is susceptible to control and does not belong to the most aggressive types of bacteria, although in that time it became out of control and caused social fear and anxiety. The anthrax preparation procedure consists of removing the liquid without destroying the chemical components of the substance. This process is similarly used in coffee production, because it preserves the taste; in the military industry, there is a chance that the bacterial spores will survive. The next step is to grind the resulting precipitate into a very fine powder. The finer the powder, the greater the chance of it later getting deep into the lungs of the victim [11]. Initially, biological weapons experts claimed that the samples looked quite primitive. The dust particles gave the impression that they had been produced in facilities with advanced technology. However, over time, experts began to change their minds - these were highly refined batches of anthrax dust, so perfect that many people believed that they must have come from the United States [11]. The reason for this conclusion is largely the belief that the chemical mixture surrounding the spores was probably prepared according to a method developed by the American military and kept a secret that no one knew about. The mixture gave the anthrax the ability to stay in the air longer and to be carried in gusts of air, such as those released by someone passing by, making the agent even more deadly [11]. Given that the technique was developed by the U.S. military, it's tempting to point at the causes of appearing antrax in the U.S. involving American laboratories.

In this context we can look at the much more dangerous "epidemic", before COVID-19 in 2020-22, which had become the AIDS illness in mid and late 80s, in comparison to the anthrax, raised a lot of doubts and justifiable fears too. Interestingly, its mortal and ruthless features and activity in the human body is almost automatically referred to – by using language of discourse of a military bio-attacks - a hidden terrorist act. Therefore Susan Sonntag writing about deadly AIDS was referring in similar way to fears of microcosm: "The invader is tiny, about sixteen thousand times smaller than the head of a pin. [...] Scouts of the immune system, large cells called macrophages when they feel the presence of a microscopic aliens immediately

notify the immune system. It starts to mobilize cell hosts, which, among other things, produce counteracts to the fight against the threat. The AIDS virus stubbornly ignores most of the blood cells in its path, avoids fast-moving defenders and traps the main immune system coordinator. At the surface of the cell, the enemy finds the receptor to which one of the proteins fits perfectly, like a key to the lock. Sticked to the cell, the virus penetrates the membrane and deprives it of the protective sheath. Then the invader locate for good in the new environment" [14] .

What scared the Americans mostly, and what aroused their particular mental discomfort, was the inability to see or visualize the enemy. An uncomfortable impotence in the ability to confront the enemy face to face. In fact, the transcendence of the anthrax germs into the field of sensory experience was decisive in the development of human imagery and fears, as the Americans themselves clearly demonstrated in their reactionary reactions. An employee of Senator Deschle's office in administration did not hide, for example, his source of anxiety because of this "miniature": "Anthrax is very scary, very frightening [...] It is invisible. [Anthrax is scary, scary because it is not visible]" [15]. He was probably convinced by the fateful comments of the scientists, who at that time poured yet more anxiety to society, such as C.J. Peters from the Texas Center for Biological Conservation. "It could infect thousands of people before anyone suspects anything is wrong. You can take out 200,000 people in a heartbeat - maybe millions. I am not worried about anthrax in the latter. I am worried about weapons of mass destruction" [13]. Quite quickly, in such a situation of uncertainty and social anxiety, the ground is created for all kinds of gossip, fakes or false alarms, which are conducive and often increase the panic and chaos. An example may be loud but false information, which was "released" by Dennis Haster' s Senator-in-Office, the spokesperson of the Senate House, that the anthrax was distributed in Capitol buildings through the ventilation system, and that afterwards all 30 employees had positive test results.

These accidents, though reproducible, can be illustrated by the often recurring mentality that comes to mind when accustomed to brutal, mechanical, and face-to-face confrontation with Western violence, freely surrendered in the face of the "biological warfare". Society had to deal with some of its aspects, in principle, when it came to the more sophisticated enemy - the microbes and the real, and more over not from the fatalistic Hollywood production. Unfortunately, these micro-robots - as viruses and germs such as HIV, Ebola, ziko, A / H1N1 ... etc. will bring many more victims before our civilization defeat them, and by the way our overwhelming, illusory modernist and scientific hopes of dealing with every untimated danger are melting down just facing dangers of microcosm. These modern and postmodern attitudes towards the micro-world are smartly commented by a mentioned before sociologist - Zygmunt Bauman: "Flies, cockroaches, spiders, mice and other "vermin" who at any time can claim their place at home without asking their legitimate residents for permission, are for this reason constantly, in every situation, "by nature" undesirable visitors ; they cannot be framed in by any schema of order, since the order is, before anything else, the state of a controlled and surrendered area. Such "self-driving" busy beings are a particular nuisance, because their peregrinations reveal something that supposed to be keep secret: the fragility, the contingency, the arbitrariness of the introduced order and the circled boundary" [16]. To confirm such Bauman's conviction let us present an example: here among the inhabitants of Western Wisconsin (specifically Northwoods place) rumors had arisen, engulfing speculative conspiracy theories. So that summer the terrain of the northern and state-of-the-wild nature was haunted by the plagues of even "black flies" (Sarcophaga aldrichi). Therefore the Department of National Resources was accused of conspiracy although the Department of National Resources's intention was to consciously propagate certain species to protect forests from verminous caterpillars, which are capable of destroying the same species of fly in their early stages of development. Probably, it turned out that the Department of Natural Resources did not predict any side effects, because, indeed, parasitic caterpillars were limited, but persistent flies remained and continued to reproduce, becoming more and more indigenous communities [17] . In that situation of fear or even trauma of bio-attacks, not only the strong columns of the Capitol were „shaken up" of the liberal-democratic order and watchfulness of the foundations of a world-wide political consensus and economic colossus, but the first of all, the social security was undermined too although the modernist model of the state had been providing security so far. As it was possible to realize that the American response to such enemy would be introducing the advanced antiseptic hygiene measures of society.

B. How American society dealt with new enemies of microcosm ?

Americans in 2001-2002 have received a dose of no longer a hyper realistic image, but real events effecting them directly. Therefore to some extent the American anthrax germs could not be treated in the American public as new representations of past fears and prejudices. Their imaginary impact was great one because it had turned out that bacteria was not capable of being killed by modern and perfect cleansers and household chemicals, and even the pharmacology initially seemed to have no certain remedy. However, struggling with a more crafty "unclean" category required a new diagnosis too. In this context professor Z. Bauman writes more on the phenomenology of microcosm agents: "But there are beings more dangerous to the order than from the "worms" themselves: such as not only wandering where they want and when they want, but in addition they do it secretly and are unnoticed. The supervisors of the order may not even realize that these micro agents have intruded into their area and that they have just nested: guardians of the order may delude themselves that the orders are not in danger – and to abandon the vigilance. Such beings ignore the established state but each question the same idea of gravity, dispelling the hope that with the right effort that one will be able to

undergo an area of charge for the good before the intruders to protect " [16].

Although not for all the destructive role of the microcosm on such a scale turned out to be sinister and surprising; They were well aware of the microscopic irresistible face of the microcosm which has long been studied by specialists and scientists. What was worse for Americans, as reported by the press at that time, in the context of problems with bioterrorism and increasingly intrusive viruses, there came up other phenomena which started to worry up larger group of people than reporters. As geneticists have said, the virus can be produced very quickly and easily, sometimes even in completely laboratory conditions [18]. It turned out also that it had been enough to download the genetic code or the whole bio-genetic project from the Internet to create a "synthetic" virus in laboratory conditions. Of course, it only applied to the models of uncomplicated genetic engineering, and therefore not to the scale of the major threat, but it probably did not help for those who had counted on limiting and eliminating bioterrorism after the post 9/11 intensification of the use of such sort of secret weapon. The instrumental use of micrology for military and terrorist purposes became a matter of common knowledge. Naturally, this is not a new thing in the history of military warfare, but the scale of the impact of the real and mental threat revealed by those who know the subject is disturbing. In addition to spectacular victims (public officials), as well as the whole atmosphere of suspicions, threat and uncertainty that surfaced after September 11, one of the major attacks and paralysis was towards the US media too.

Attack on American media caused discomfort and social disappointment because the American media, apart from being an obvious key tool for communication – were taken as an area of the immune circulation of all information and the maintenance of interpersonal relations as well. Moreover media are the condensed center of all simulacra - which multiply the reality, the spectacular area like matrix cords to which society is attached for 24/7. First of all, the media are, however, considered to be a basic political and moral training ground, and as a result, during the crisis, it is a strategic weapon of destruction - even in the mind of Jean Baudrillard's very perceptive observation: "Americans generally use two types of weapons: aviation and information. They therefore carry out a two-pronged attack, consisting in physical bombing of the rest of the world. Both the air force and the power of information belong to superterritorial weapons …." [19].

Direct bio-attacks (apparently of course perpetrated by terrorists) were indirectly treated as a threat to the freedom of information exchange, and on the other, as a disturbing attempt to anticipate possible counterattack from the side of the U.S. Perhaps they also felt the aggression on the fourth so called social power. It turned out that they were the special victims and at the same time the primary targets of the bio-attacks. If we do research of American press releases from that time, we have a clear picture of the backdrop of American media. It should be highlighted that the first victims of the anthrax, also mortal, were workers of significant media sources. Let us outline shortly this calendar of main, decisive accidents: the death of Robert Stevenson, a 63-year-old photographer of the tabloid The Sun in Boca Raton, Florida, was presumably caused by ignoring the symptoms of anthrax infestation. That first death at the very beginning did not generate any major suspicions. But soon it turned out that the employee (Ernesto Blanco) who was responsible for correspondence in the press American Media Inc. fell into a similar illness, and further - five other corporate colleagues got positive test results. After those cases came up a panic, but there was also a change of the center of the suspicions from New York moved to the American capital - Washington D.C. In the light of the media there were such victims: Erin O'Connor, working for a famous news anchor Tom Brokaw in the New York branch of the NBC station, is getting a skin infection, a 7-year-old son of ABC News producer is subjected to antibiotic treatment due to skin infection [20]. More and more suspicious shipments and envelopes with dangerous "powder" were also found addressed inadvertently to strangers. Probably there were not many of them before, but bigger number of controls generates the atmosphere of danger. Also suspicious, the white powder finally came to the editor of Dan Rather, who became almost a media hero from unforgotten Tuesday of September 11th, 2001, when he was the frontline face of ABC TV Channel News reporting dramatically terrorist Tuesday's events (9/11) in the eyes of America as a symbol of American power, resistance and courage. He confirmed his stance on the talk show with David Latterman when, perhaps just for the first time in the history of this iconic nightly talk show of ABC instead of irony and joke, there were showed genuine emotions and tears. Therefore when the threat of anthrax reached Rather's office and his person, Americans realized that situation was becoming very serious. Ordinary Americans were getting upset because they have had enough of some obscure speculation; clearly, they were suspecting Al Qaeda's revenge against American media for being too active and engaged in the verdicts made by some courageous journalists and media representatives (Dan Rather casus). There were also other locations of bioterrorism of using anthrax in America of post 9/11 time - like the next case of a correspondent for American Media Inc., 36-year-old Stephanie Dailey. Sooner or later further events were touching the world of politics through the institutions of the national mail office after the loud closure of the six rooms of the Capitol Congress on the orders of the US President.

The obsession of fear was so intense that it included the size of the publishers of thousands of low and high-volume writers, including those of provincial institutions or people involved in other types of media activity. American feelings were experiencing in 2002 and in the previous year their worst moments, but in the same time also stimulated "resourceful" Americans, prompting them to a sharp rush to provide themselves inevitable secure means and secure themselves for the future. American society reached the peak of social fear of potential bio-attacks when the administrators of the city skyscrapers started to buy parachutes (for example such unconventional equipment,

which could be opened much faster than the traditional ones, and which allowed a jump from 30-35 feet [range of 10 floors], and costed $ 795, even more all kinds of gas masks (Evac-U8 for eg. 69.95 $), antibacterial overalls, for sophisticated inventions to protect against unexpected terrorist bio-attacks. Another significant impact of panic on health policy at that time was not only evidenced by the increased use of pharmaceuticals. Fear of the use of nerve gas also led to the unnatural acquisition of gas masks, even though a gas mask does not guarantee certain survival in the event of a gas attack. These cases prove again that the post 9/11 anti-terrorist hysteria in USA has created artificial consumer needs.

IV. Conclusions

The symbolic meanings of the microcosm mentioned at the beginning referring even to Nazi German and Soviet, totalitarian rhetoric: worms, insects, bacteria or viruses, were also marked in the American media after 9/11 with heavy and pejorative meanings that connoted the enemies, war, terrorists or attack.

Rational, even exaggeratedly practical American approach to many issues, which easily provokes mockery and irritates Europeans, is undoubtedly rooted in the cultured model of the modern state, cultivated for centuries and fetishized. Different descriptions of such behavior are diagnosed by different means of description. Firstly, we were able to see in these mentioned, artificially induced consumer needs, released by the mechanisms of liberal economics according to the specific functioning of the American state in the determinate potentials of combined a need and supply. In American commercialization of almost every thing even human tragedies and death, pain and less positive experiences have been not excluded from this "divine" legitimacy of making profits, there was nothing wrong with that according to the American protestant-bourgeois mentality. In spite of fear or tragedy, some companies must ultimately generate profits. Another possible sociological approach to such a kind of forward thinking is the George Ritzer theory of McDonaldization, which also has been to some extent reductive in wanting to see the spectrum of functioning of American society within just expansive governing paradigm: efficiency, predictability, calculation and planning [20]. After all, the influence of McDonalds model especially predictability and planning, is being influenced on a daily basis. Americans do not disdain of preparing and serving meals, work organization, science, health, administration or leisure because everything is important and can become worthy also from the economic point of view. The United States belong to a group of countries based on an extremely developed and complex set of insurance systems - which is probably the effect of rational, legal regulation, so in this context of predictable and preventive approach of American society the tragic events of September are even more merciless for those who were unwilling to insure themselves in advance unfortunately perished under the WTC ruins, no mentioning that they were mostly immigrants who paid double price in this tragedy. Unfortunately in those surroundings of cult of formalism and bureaucratic, clerical discipline, there was not much place for human sentiments; a such attitude is to some extent derived from Max Weber's "awe-inspiring rationality" and used to be taken somewhat as a threat which motivates people. In addition next to the economic motive of American predictability, one should also mention the whole essential because of the mental paradigm of which G. Ritzer comments: rationalization requires a lot of effort to ensure that everything is going as it should. This is why rational society respects and emphasizes discipline, order, systematization, formalization, routine, consistency and methodology of behavior. In such society most of people like to know what are they going to expect in a moment. They do not want to and do not expect too many surprises [21].

In the reviewed cases of American reactions to bio-attacks after 9/11, the new technologies also had a transformative effect on the way how foreign news was covering the events. Today entering the wildly revealing era of the “eco-system,” in which undefined, unfiltered news are circulating by cell phone or WhatsApp. Therefore since then, media were more controlling power, cell phone quickly acquired the awesome power of a tanks, which could create the revolutions and even collapses of governments as the instances of the Arabic Spring. The post 9/11 period in America media was one of such narration, big, important, damaging in its impact, but hopefully instructive for the questions it raised for the nation’s consideration. One such question revolves around the deepening politicization of the media.

Since 11/9 no doubt, that the news magnified the administration’s terrorism alerts by reporting such announcements mostly in lead stories and very long segments, while downplaying the new lower alert levels or not covering such changes at all. Bacteria, worm and insects are used not only to symbolize strangers but mostly in political discourse they are exploited by politicians and common people as well to frame other politicians or opponents as a enemy. It is not only issue of the past but a current tool of meaning.

Viruses, germs, bacteria or other pathogens, as semiotic and symbolic prolongation of the threat of "foreigners", aliens, especially terrorist forces, circulated not only over the images of the WTC ruins, barely covering them in October 2001. In these days, when the traumatic tragedy has been tamed or dismissed, there will be other micro-threats and fears that threaten the behaviour of politicians or candidates for the White House. Perhaps the postulated by president Donald Trump's to build wall on the southern border with Mexico will begin to play an additional role with the Brazilian Ziko virus, transmitted by specific mosquitoes, and the Latino immigrant will be marked by another stereotype. Microcosms like an epidemics will be cyclically returning as the book of modern beasts of our time.

REFERENCES

[1] M. Kawa, Ten, który toczy nasze dusze i ciała... Robak i robactwo w kulturze i literaturze. Toruń: Wydawnictwo Adam Marszałek, 2011. pp. 20-21.

[2] J. Amato, Dust. A History of the Small and the Invisible, Berkeley and Los Angeles: University of California Press. 2000, pp. xii, 250.

[3] D. Macdonald, „Teoria kultury masowej". In. Wiedza o kulturze. Antropologia kultury, A. Mencwel, Ed. Warszawa: 1992, p. 480.

[4] J. Trachtenberg, Diabeł i Żydzi. Średniowieczna koncepcja Żyda a współczesny antysemityzm, Gdynia: 1997, p. 55.

[5] Z. Bauman, „O nowoczesności TEJ Zagłady – raz jeszcze," In. Kultura Współczesna. Vol. 2, p. 121, 1993.

[6] L. Smolka, „Symbolika polsko-niemieckiego obrazu wroga doby powstań i plebiscytu Górnośląskiego". In. Wokół stereotypów Niemców i Polaków, W. Wrzesiński ed. , Warszawa: 1993, p. 219.

[7] K. Liszowski, Wojna polsko-sowiecka 1939, Londyn: 1986, p. 312.

[8] A. Karlen, Człowiek i mikroby, transl. G. Siwek, Warszawa: 1997, pp. 255–256.

[9] Common Knowledge, eds. W. Russell Neuman, Martin R. Just and Ann N. Crigler. Chicago: 1992. University of Chicago Press, p. 2.

[10] J. Kass, Chicago Tribune, p 2. Wednesday 13, September, 2001.

[11] P. Moore, Tajemnicze choroby współczesnego świata. Nowe zagrożenia, wirusy, bakterie, zarazki. Warszawa: Wyd. Bellona, 2009, p. 125.

[12] D. Glanton, "West Nile kills 2 more in Louisiana", In. Chicago Tribune, Vol. 10, 2002, Saturday 10 August, p. 10.

[13] These and other information we took from the series of articles in "ChicagoTribune ", no. 291, pp. 1, 12, 14-15. October 18, 2001.

[14] S. Sontag, Choroba jako metafora. AIDS i jego metafory, transl. J. Anders, Warszawa: 1999, ed. PIW, pp. 104–106.

[15] S. Sternberg, "Making anthrax a weapon is hard", USA Today, Vol. October 18, p. 2A. 2001.

[16] Z. Bauman, Ponowoczesność jako źródło cierpień, Warszawa: ed. SIC!, 2000, p.14.

[17] [17] D. Holt, "Conspiracy theory, Wisconsin by Sworm," Chicago Tribune, Saturday 7, pp. 1-13, July, 2002.

[18] P. Roser, "Study: virus can be made with ease," Chicago Tribune, Friday 12 p. 11, July, 2002.

[19] J. Baudrillard, Ameryka, transl. R. Lis, Warszawa: ed. SIC!, 2001, p. 67.

[20] S. Kapos, "Amid fear, some firms see profits", Chicago Tribune, vol. 291, p. 8, October 18, 2001.

[21] G. Ritzer, Mcdonaldyzacja społeczeństwa, transl. S. Magala, Muza Ed. Warszawa, 1999, p. 145.

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 127-133

Electronic Attack Using SDR

Ivan Ivanov
C4I Systems Development Directorate
Defence Institute "Prof. Tsvetan Lazarov"
Sofia, Bulgaria
i.p.ivanov@di.mod.bg

Sevdalin Spassov
C4I Systems Development Directorate
Defence Institute "Prof. Tsvetan Lazarov"
Sofia, Bulgaria
s.spasov@di.mod.bg

Abstract: **The essence and main characteristics of electronic attack (EA) are examined, as well as its place in the electronic warfare (EW). The main elements of EA are examined, such as jamming, spoofing and electronic neutralization of enemy radio devices. A definition and the main terms for software-defined radio (SDR) are given. The architecture and main characteristics of SDR are examined. A prototype of SDR is made and demonstrated for the purpose of proving the concept.**

Keywords: electronic warfare, electronic attack, GNU radio framework, software-defined radio.

I. INTRODUCTION

Over the past three decades of persistent conflict, the opposing forces had used its most capable communications systems ever. During this time, the most powerful armies have continued to dominate the electromagnetic spectrum over the enemies and adversaries who lack the ability to challenge their technological superiority. However, in recent years, regional peers have demonstrated formidable capabilities in hybrid operational environments, including electromagnetic spectrum. These capabilities have been also demonstrated in the ongoing conflict in Ukraine mainly in the form of jamming of communications, global navigation satellite system (GNSS) and control systems of military drones.

All combat platforms are being built with a wide application of electronic devices and systems. A large part of these systems receives and transmit both data and control signals. These data and signals are transmitted and received using electromagnetic waves. The use of the electromagnetic spectrum makes them vulnerable to interference by the enemy. All this assumes the growing importance of electromagnetic warfare in recent military conflicts. US Air Force and US Department of the Army use the term Electromagnetic Warfare (EW) [1], [2]. NATO uses the term Electronic Warfare in some doctrinal documents [3], but has changed it to Electromagnetic Warfare in the recent documents [4]. The Electromagnetic Warfare has been adopted as a main term in this paper and it is used in the entire text. Electromagnetic Warfare is one of the main warfare domains. When conducting all electromagnetic warfare activities, it is necessary to receive, digitally process, analyse and store radio signals in a wide frequency range. In addition, in order to conduct an electromagnetic attack, it is necessary to synthesize jamming signals with different parameters, after which they can be emitted in several frequency ranges. All technical activities such as reception, digital processing, analysis and synthesis of signals can be performed using software-defined radio (SDR). The possibilities of applying SDR in electromagnetic attack systems, as well as an exemplary prototype of such a system, are discussed further in the article.

II. MATERIALS AND METHODS

A. Main characteristics of Electromagnetic Attack (EA) and its place in Electromagnetic Warfare (EW).

Electromagnetic warfare [1], [2] is the use of electromagnetic energy to provide situational awareness and achieve offensive and defensive results, and to ensure superiority in the electromagnetic spectrum. EW consists [1] - [4] of three main elements (Fig. 1).

The three main elements of the EW are Electromagnetic Attack (EA), Electromagnetic support (ES) and Electromagnetic Protection (EP). The adjective Electromagnetic replaces adjective Electronic in the recent EW conceptual documents. These three elements are inextricably linked, as they are mutually dependent and are applied in a certain sequence. For example, information about the parameters of radio signals and the location of enemy radio assets, acquired by electromagnetic support, is used to synthesize jamming signals emitted by the transmitters of the electromagnetic attack.

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8483
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

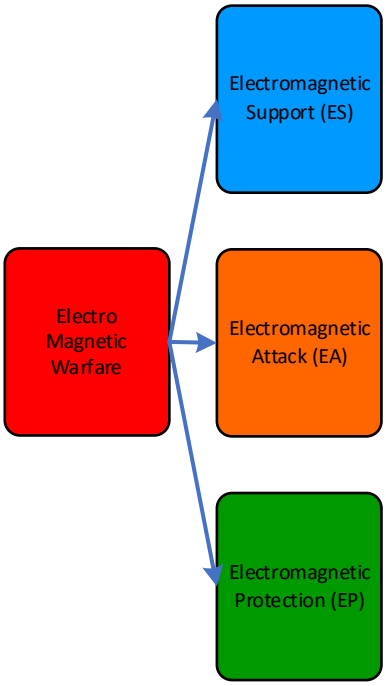


Fig. 1. Elements of the Electromagnetic warfare.

Electromagnetic attack is one of the three main elements of electromagnetic warfare. Electromagnetic attack consists of three main elements: electromagnetic jamming (EJ), electromagnetic deception (ED) and electromagnetic neutralization (EN).

Electromagnetic support (ES) is a component of electromagnetic warfare, which includes actions to search, intercept and identify electromagnetic emissions and locate their sources, in order to immediately recognize the threat and build situational awareness. It provides a source of information necessary for immediate decision-making for electronic countermeasures [5] and other tactical actions.

Electromagnetic Protection (EP) is a complex of technical and organizational measures using electromagnetic energy to provide protection and effective use of the electromagnetic spectrum by allied forces, carried out in order to ensure the stable operation of their own systems and means of controlling troops and weapons, in conditions of electronic effects from the enemy. Electromagnetic protection is divided into active and passive. Active electromagnetic protection is a complex of measures that can be revealed by the enemy, such as - a change in the parameters of the transmitter to such an extent as is necessary to ensure the effective use of the electromagnetic spectrum. Passive electromagnetic protection is a complex of measures that remain hidden from enemy intelligence, such as - operational procedures and reducing their own radiation (signature) in different frequency ranges of EM waves. For example, in the radio frequency range, technical and constructive measures are applied to reduce the effective reflecting surface (RCS - radar cross section) of their own combat platforms - these are the so-called STEALTH technologies. Similar measures are taken to reduce emissions from combat platforms in the infrared (IR), visible, ultraviolet (UV) and sound ranges. Conducting EW involves several processes, combined into the two main cycles shown in Fig. 2.

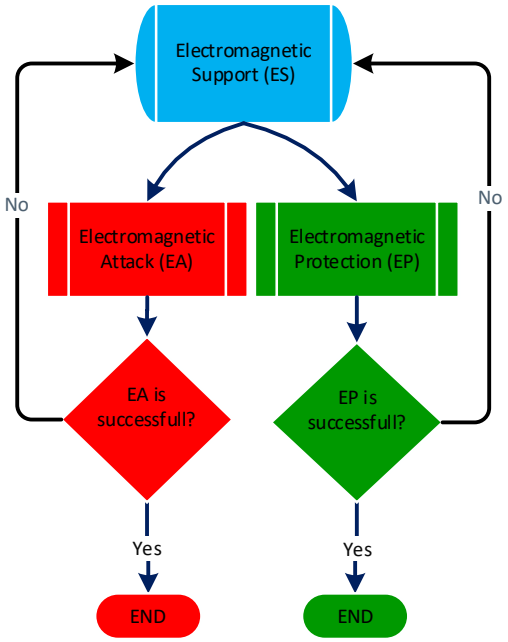


Fig. 2. Processes in the EW.

EW begins with Electromagnetic Support (ES) actions: searching, intercepting and identifying electromagnetic emissions and locating their sources. This information then is used to initiate actions, organized in two cycles: electromagnetic protection and electromagnetic attack. Electromagnetic Protection (EP) includes a set of technical and organizational measures for protection and sustainable operation of the own electronic systems and for the effective use of the electromagnetic spectrum by allied forces. These actions are carried out in order to ensure sustainable control of weapons in conditions of radio-electronic jamming by the enemy. At the end of this cycle of actions, it is checked whether the electromagnetic protection has achieved its goal. If the goal is achieved, then the electromagnetic protection actions stop, and if the goal is not met, the electromagnetic protection actions begin again and the cycle repeats. The electromagnetic attack is organized in the second cycle. It also uses the results of the electromagnetic support, which determines the parameters of the received enemy radio signals and their sources. Jamming signals are emitted to the enemy using electromagnetic attack devices. At the end of this cycle of actions, it is checked whether the electromagnetic attack has achieved its goal. If the goal is achieved, then the electromagnetic attack stops, and if the goal is not achieved, then the parameters of the received enemy radio signals are again determined using the electromagnetic support and the cycle repeats. This type of functioning of the system is called reactive jamming.

The essence, elements and main characteristics of the electromagnetic attack (EA)

Electromagnetic attack includes actions to prevent or reduce the effective use of the electromagnetic spectrum by the enemy through the use of electromagnetic energy. EA is expressed in:

– actions aimed at preventing or reducing the effective use of the electromagnetic spectrum by the enemy, such as suppression of radio transmission or electromagnetic deception;

– use of weapons that use electromagnetic or directed energy such as lasers, radio frequency weapons, particle radiation, etc.;

– offensive and defensive actions including countermeasures.

Electromagnetic attack includes two types of actions: offensive and defensive. Defensive actions use the electromagnetic spectrum to protect personnel, facilities, capabilities and equipment. Examples of defensive actions include protective measures such as: active jammers, countermeasure systems using infrared directed energy, countermeasures against unmanned aerial systems (C-UAS). Offensive EA prevents or reduces the effective use of the electromagnetic spectrum (EMS) by the enemy by using electronic jammers and directed energy weapons systems against enemy systems receiving EM waves in the radio frequency and electromagnetic spectrum. Electromagnetic attack [1] includes three main elements as shown on Fig. 3:

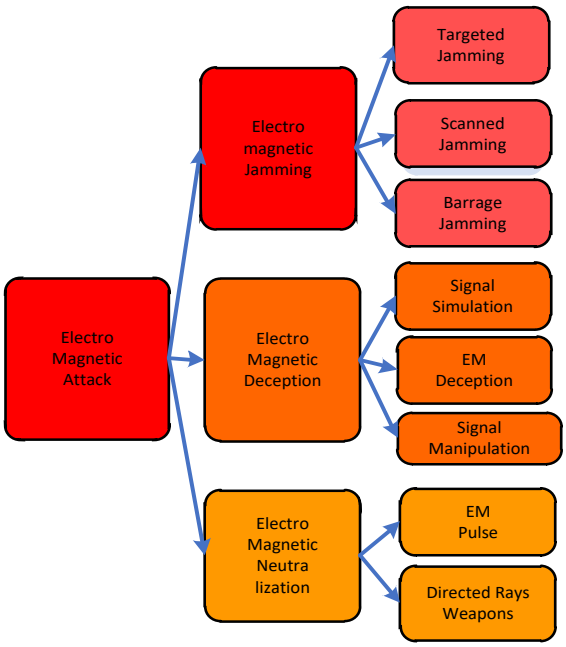


Fig. 3. Components of the electromagnetic attack

– Electromagnetic jamming (EJ),
– Electromagnetic deception (ED) and
– Electromagnetic neutralization (EN).

The general form of EA involves detecting and identifying enemy targets, and conducting activities to gain superiority in the electromagnetic spectrum. In addition, electromagnetic attack actions include a variety of electromagnetic deception techniques, such as false targets or the creation of duplicate targets. Directed energy can be defined as a concentration of electromagnetic energy or atomic and subatomic particles. Directed energy weapons use it as a means of damaging or destroying enemy assets, systems, equipment, and personnel. In addition to their destructive effects, directed energy weapon systems maintain the isolation of areas and control of large groups of people.

Electromagnetic jamming (EJ) is the deliberate emission, secondary emission, or reflection of electromagnetic energy to reduce the effectiveness of enemy electronic devices, equipment, or systems. Examples of offensive actions include jamming enemy radars or electronic command and control systems and the use of anti-radar missiles to suppress enemy air defence assets.

Electromagnetic deception (ED) by electronic means is the deliberate emission, secondary emission, modification, absorption, or reflection of electromagnetic energy in a manner intended to confuse, destroy, or divert an adversary or its electronic systems from proper operation.

Electromagnetic neutralization (EN) is the deliberate use of electromagnetic energy to temporarily or permanently damage adversary devices that rely exclusively on electromagnetic radiation for their operation [3]. Electromagnetic neutralization typically results from the use of directed energy or a beam from a device possessing sufficient electromagnetic energy at a target to temporarily or permanently disable the target, its electronics, or both. The use of lasers to blind people or to destroy sensitive optical devices are two such examples. The considered classification of the elements of the electromagnetic attack is according to the type of emitted jamming signals. If the electromagnetic attack is considered from the point of view of the object of the attack, then several types of jamming signals are determined. These are jamming signals for enemy radars, for communication networks, for reconnaissance radio systems, for other combat platforms. A good study of electromagnetic attacks on wireless communication networks have been done in [7].

B. General information about software-defined radio (SDR)

Software-defined radio is a modern paradigm for the practical implementation of radio communication systems. The foundations of the “software-defined radio” (software-defined radio - SDR) paradigm are associated with the research of DARPA and the US Air Force under the SpeakEasy project in the early 1980s on the creation of a prototype radio station covering the range from 2 MHz to 2 GHz and implementing about 10 communication standards [8]. Part of the results obtained in the field of system architecture were published by Mitola in the early 1990s, where the author [9] introduced the concepts [10] “software radio” and “software-defined radio” [11]. Each professional organization attempts to

define a common framework of terms and definitions to allow for easy communication among professionals working in a common field. In the field of software-defined radio communications, the Institute of Electrical and Electronics Engineers (IEEE), through its working group P1900.1, has created definitions (Table I) to ensure that everyone in the field has a common terminology [12]. A key definition in this brief ontic is that of "software-defined radio": a radio in which some or all of the physical layer functions are software-defined.

The definitions introduced allow not only to standardize the concept of SDR, but also to create a context in which this concept "lives". This allows the formation of other contexts in which SDR can be attributed to different entities.

A structural-functional block diagram of such a radio is shown in Fig. 4.

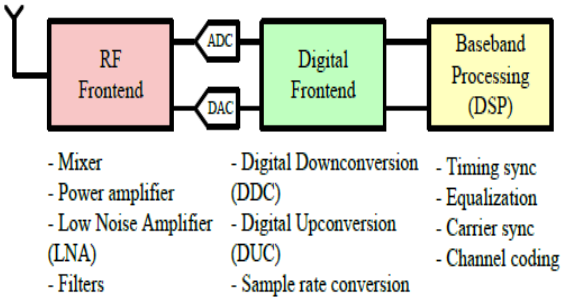


Fig. 4. Software-defined radio architecture

One of the main differences between the architecture of a software-defined radio and an ideal one is the presence/need of a radio frequency front-end operating in the analogue space and implementing such functions as mixing, low-noise amplification, analogue filtering, etc. Another architectural feature of modern SDRs is the implementation of digital processing by two digital blocks – a digital front-end and a baseband digital signal processing block. The first block performs all conversions from transmitted to baseband (and vice versa) and those related to the clock frequency (frequency compression, expansion, etc.). The second block performs all conversions to baseband and is typically implemented by a general-purpose computer or a single-board microcomputer.

TABLE I ONTIC OF CONCEPTS IN THE FIELD OF SOFTWARE-DEFINED RADIO COMMUNICATIONS

Concept	Definition
Radio	1. A technology for the wireless transmission or reception of electromagnetic signals enabling the transfer of information. 2. A system or device incorporating technology as defined in (1). 3. A general term applied to the use of radio waves.
Radio Node	A radio point of presence, including a transmitter and/or receiver.
Software	Modifiable instructions executed by a programmable processing device
Physical	The layer within a wireless protocol that processes radio frequency (RF), intermediate frequency (IF), or baseband signals, including performing channel coding. It is the lowest layer of the 7-layer ISO model adapted for wireless transmission and reception.
Data Link Layer	The protocol responsible for the reliable transmission of frames over a wireless link by using appropriate error detection and control procedures and media access control.
Software Controlled	Software control refers to the use of software processing in the radio system or device to select operating parameters.
Software Defined	Software-defined refers to the use of software processing in the radio system or device to perform operational (but not control) functions.
Software Controlled Radio	A radio in which some or all of the physical layer functions are software controlled.
Software-Defined Radio	**A radio in which some or all of the physical layer functions are software defined.**
Transmitter	Equipment producing radio frequency energy for radio communication purposes.
Receiver	A device that receives a radio signal and provides information extracted from it.
Air Interface	A subset of waveform functions designed to establish communication between two radio terminals. This is the equivalent of the wireless physical layer and wireless data layer waveforms.
Waveform	1. The set of transformations applied to the information to be transmitted and the corresponding set of transformations to convert the received signals back to their information content. 2. Representation of the signal in space. 3. Representation of the transmitted radio frequency signal plus additional radio functions, including all network layers.

The analogue RF front-end, ADC, DAC and digital front-end are combined into a common building block – RF digital front-end in current products on the market that allow prototyping in the field of SDR. This leads to the generalized, mass, modern SDR architecture shown in Fig. 5.

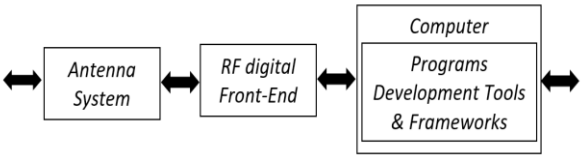


Fig. 5. Generalized mass architecture of SDR.

Table II summarizes the main characteristics of popular radiofrequency front-ends used to build SDRs.

The analysis of the data in Table 2 shows the availability of capabilities for supporting a wide frequency range – a part of HF, VHF and UHF, a wide bandwidth of the processed radio channel – up to 120 MHz. There is availability of transmitting/receiving a high data exchange speed with personal computer platforms – up to 10 GBit/s and to support of multiple coherent radio channels, etc.

These characteristics allow the implementation of variety technologies such as GSM, LTE, DVB, FMCW Radar, MIMO, etc.

TABLE II MAIN CHARACTERISTICS OF POPULAR RADIOFREQUENCY FRONT-ENDS FOR SDRs

Plat-form	Frequ-ency range	Channel band-width	Digital conver-ters bit resolution	Digital interface	Radio channel number
Hack RF One	10 MHz - 6GHz	20 MHz	8 bit	USB 2.0	1 Rx/1 Tx
Adalm PLUTO	325 MHz - 3.8 GHz	20 MHz	12 bit	USB 2.0	1 Rx/1 Tx
Ettus B210	70 MHz - 6 GHz	56 MHz	12 bit	USB 3.0	2 Rx/2Tx
Ettus N210	10 MHz - 6 GHz	40 MHz	14-bit ADC 16-bit DAC	1G Ethernet	2 Rx/2Tx
Ettus X210	50 MHz - 2,2 GHz 400 MHz - 4.4 GHz 1.2 GHz - 6 GHz	120 MHz	14-bit ADC 16-bit DAC	10G Ethernet, PCIe	2 Rx/2 Tx, 4 R x
Ettus X310	10 MHz до 6 GHz	160 MHz	14-bit ADC 16-bit DAC	10G Ethernet, PCIe	2 Rx/2 Tx, 4 Rx
Lime SDR	100 kHz - 3.8 GHz	61.44 MHz	12 bit	USB 3.0	6 Rx/4 Tx
Pico SDR	70 MHz - 6 GHz	56 MHz	12 bit	PCIe	4 Rx/4 Tx 8 Rx/8 Tx
RTL-SDR	24 – 1766 MHz	3.2 MHz (2.4 MHz typical)	8 bit	USB 2.0	1 Rx

The SDR technology is supported by numerous software packages for computer modelling and simulation. The most famous of them are: Matlab, GNU Radio, LabVIEW, etc. The advantage of using such packages is the rapid transition from a computer module to a practical implementation.

III. RESULTS AND DISCUSSION

An electromagnetic attack on a Wi-Fi network can be done by SDR by three general concepts. The first of them is to perform electromagnetic jamming, the second one relies on the electromagnetic deception and the third uses electromagnetic neutralization.

A prototype of an electromagnetic jamming system based on software-defined radio has been created in order to proof the first concept. The test scenario is shown at Fig. 6. It includes a mobile device, a Wi-Fi access point and attacking device (jammer), performed by SDR. The Wi-Fi wireless network was chosen, based on its popularity and availability.

SDR functions as a jammer that disrupts the radio connection between a Wi-Fi network access point and a mobile device. The test scenario examines the impact of different jamming types on radio connection between a Wi-Fi network access point and a mobile device.

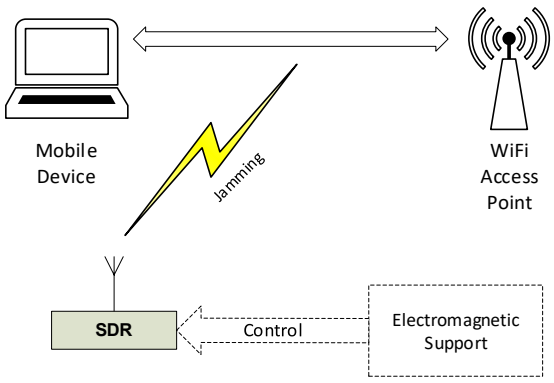


Fig. 6. The Test scenario.

System realization of SDR as a jammer is shown at Fig.7 consisting of the X310 front end, power amplifier and the GNU radio software package.

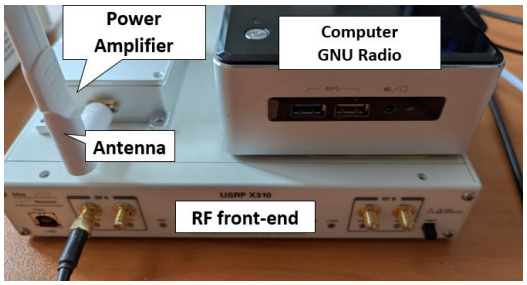


Fig. 7. Implementation of SDR for EA.

The radio framework flow graph of SDR for EA, based on a GNU radio software package is presented on Fig. 8.

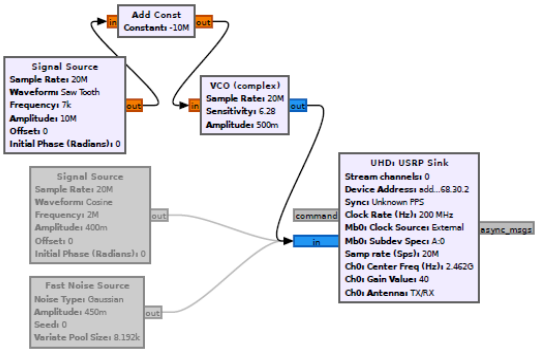


Fig. 8. GNU Radio Framework flowgraph of SDR for EA.

The mobile device has established a stable radio connection with the Wi-Fi network access point. With the help of Electromagnetic Support, the main parameters of the radio network have been determined and submitted to the electromagnetic attack system. The spectral waterfall

diagram of normal Wi-Fi activity on targeted channel is presented on the Fig. 9.

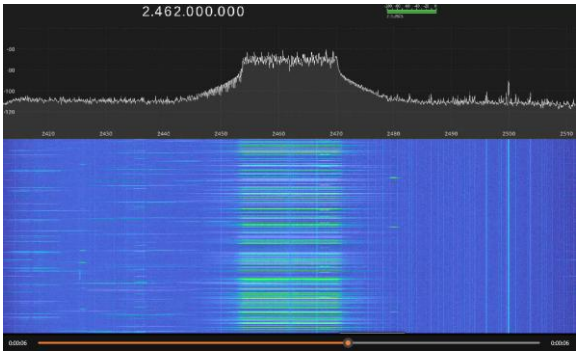


Fig. 9. A spectral waterfall diagram of Wi-Fi activity on targeted channel.

Two types of jamming signals have been generated in the GNU radio environment. These jamming signals have the same radiated power, but have different bandwidths. The first signal is a barrage radio jamming in the entire width of the Wi-Fi network bandwidth of 20 MHz. The second signal is a narrowband jamming that scans the entire width of the Wi-Fi radio network bandwidth.

Two experiments have been conducted in a controlled, rather than public, environment to avoid risks of violating legal and ethical requirements. The result of the impact of electromagnetic jamming on the radio connection between the mobile device and the Wi-Fi network has been evaluated. The desired effect is to achieve a failure in the performance of a basic function in the targeted Wi-Fi radio network, such as a lack of communication between the access point and the mobile device.

The results of the experiments are shown on the Fig. 10 and Fig. 11. The waterfall view of the barrage jamming on the Wi-Fi radio connection is shown on Fig. 10. It covers the whole Wi-Fi radio bandwidth by almost equal power of the jamming.

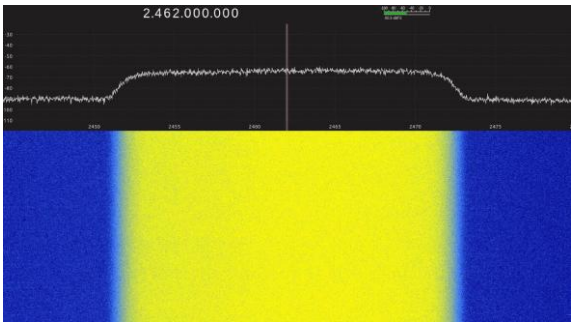


Fig. 10. The barrage jamming on the Wi-Fi radio connection.

The waterfall view of the second disturbance signal - scanned jamming on the Wi-Fi radio connection is shown on Fig.11.

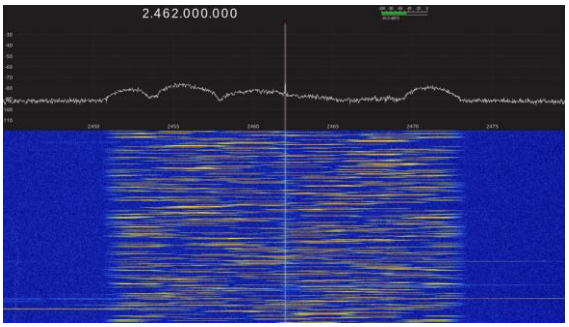


Fig. 11. The scanned jamming on the Wi-Fi radio connection.

A low-speed scanned jamming has been used in the entire Wi-Fi channel passband. The scanned jamming covers almost the whole network bandwidth by noise with fluctuating power, visible in Fig. 11. The power of the scanned jamming isn't uniform distributed across the entire frequency band of the Wi-Fi radio network. This is a weakness of frequency-scanning jamming. To achieve denser coverage of the entire Wi-Fi channel bandwidth, the frequency change of the scanned jamming must be increased.

The searched effect - lack of communication in the targeted Wi-Fi radio network has been achieved. These results validate the concept in Fig.6.

The second way to make electromagnetic attack on a Wi-Fi network can be done by means of electromagnetic deception (ED). An example of a GNU Radio Framework flowgraph of SDR Wi-Fi transmitter performing ED is shown on Fig. 12. By the GNU Radio block "WiFi MAC" SDR pretends as the access point (AP) and constantly addressing the mobile device. Preliminary results of degradation of the communication was achieved as a validation of the concept.

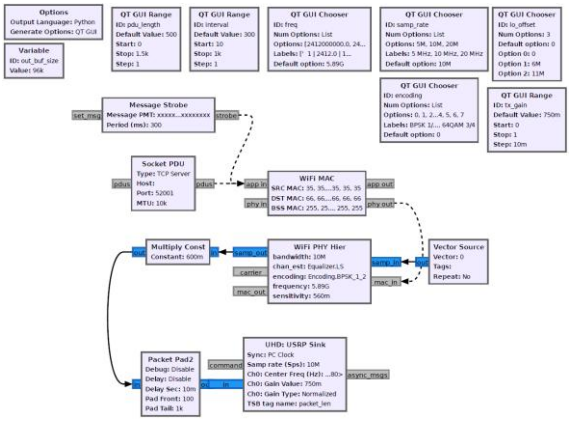


Fig. 12. GNU Radio Framework flowgraph of SDR Wi Fi transmitter performing ED.

There are numerous limitations, challenges, and risks associated with the application of SDR to EA. It is a challenge for an SDR to simulate an access point and overload the targeted mobile device by continuous addressing and data flow. There are a number of limitations, such as simulating a real data stream for the purpose of deception and transmitting it over the Wi-Fi

radio network to the end mobile device. There is also a risk of improper jamming of public Wi-Fi radio networks if the experiment is conducted in a controlled environment that is close to such radio networks. All these limitations, challenges, and risks associated with the application of SDR to EA have to be considered in the future experiments.

IV. CONCLUSIONS

Two approaches are considered for implementing an electromagnetic attack with SDR on a WiFi radio network.

The first approach involves electromagnetic jamming. A prototype of an electromagnetic jamming system based on software-defined radio has been created in order to proof the concept. Two types of jamming signals have been generated in the GNU radio environment - a barrage radio jamming and a scanned jamming in the entire width of the Wi-Fi network. The barrage jamming on the Wi-Fi radio connection jams the whole Wi-Fi radio bandwidth by almost equal power on each frequency. Compared to it, the scanned jamming signal hasn't uniform power distribution across the entire frequency band of the Wi-Fi radio network. The power distribution of the scanned jamming depends of its sweeping speed.

The desired effect - loss of basic function such as lack of communication in the targeted Wi-Fi radio network – has been achieved in both experiments. Additional experiments are to be conducted in various real-world conditions to compare the impact of barrage jamming and frequency-scanned jamming on Wi-Fi radio networks.

The second approach to make electromagnetic attack on a Wi-Fi network can be done by means of electromagnetic deception. An example of a GNU Radio Framework flowgraph of SDR Wi-Fi transmitter performing ED has been done. No experiments have been conducted yet in real conditions to assess the impact of electromagnetic deception on Wi-Fi radio networks. Field tests should be done in a controlled environment and in various real-world conditions to prove this concept and to assess the impact of this jamming on Wi-Fi radio networks.

ACKNOWLEDGMENTS

This work was supported by the NSP SD program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement № Д01-74/19.05.2022.

REFERENCES

[1] Department of the Army, "FM 3-12: Cyberspace operations and Electromagnetic Warfare", US Army, August, 2021. Available: https://irp.fas.org/doddir/army/fm3-12.pdf. [Accessed: Feb. 04, 2025].

[2] US Air Force, "Air Force Doctrine Publication 3-85: Electromagnetic Spectrum Operations", US Air Force, Dec. 14, 2023. Available: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-85/AFDP%203-85%20Electromagnetic%20Spectrum%20Ops.pdf. [Accessed: Feb. 05, 2025].

[3] NATO, "AAP-06: Glossary of terms and definitions", NSO, 2021. Available: https://standard.di.mod.bg/pls/mstd/f?p=600:1:8391929042894131. [Accessed: Feb. 05, 2025].

[4] NATO, „Electromagnetic Warfare", Mar. 22, 2023. [Online]. Available: https://www.nato.int/cps/en/natohq/topics_80906.htm. [Accessed: Feb. 05, 2025].

[5] S. Spassov, K. Paraskov, P. Kokudeva, J. Petrov, Concept of use and operational requirements for passive defense software-defined radar systems: ARTDEF Conference, November 28-29, 2023, Sofia, Bulgaria. Sofia: BDI Acad. Publishing, 2024.

[6] H. Pirayesh and H. Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey", IEEE Communications Surveys & Tutorials, vol. 24, Issue: 2, pp. 767 – 809, Secondquarter 2022.

[7] NATO, "Allied Joint Doctrine for Electronic Warfare", NATO Standard AJP-3.6, March 24, 2020.

[8] R. J. Lackey and Donald W. Upmal, "Speakeasy: The Military Software Radio", IEEE Communications Magazine, vol. 33, Issue 5, pp. 56 - 61, May 1995.

[9] J. Mitola III, "Software Radios: Survey, critical evaluation and future directions", IEEE Aerospace and Electronic Systems Magazine,Vol. 8, Issue 4, pp. 25 – 36, April 1993.

[10] J. Mitola III, "The Software Radio Architecture", IEEE Communications Magazine, vol. 33, Issue 5, pp. 26 - 38, May 1995.

[11] A. Margulies and J. Mitola III, Software Defined Radios: A Technical Challenge and a Migration Strategy: IEEE 5th International Symposium on Spread Spectrum Technologies and Applications, September 2-4, 1998, Sun City, South Africa. Piscataway NJ: IEEE Service Center, 1998.

[12] A. Wyglinski, T. Collins, D. Pu, and Robin Getz, Software-Defined Radio for Engineers. Norwood, MA, Artech House, 2018.

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 135-139

Research of the Energy Status of Military Personnel During Complex Tactical Exercises

Krasimir Koynakov
Logistics and Tehnology department,
Vasil Levski National Military
University Veliko Turnovo, Bulgaria
Krasi.koynakov@gmail.com

***Abstract*— This paper presents a study among cadets from the Vasil Levski National Military University of their energy status during complex tactical exercises. Their energy intake and energy expenditure were studied, using the methods of tabular timing and food intake history. The values of the studied quantities were compared with the national physiological norms for nutrition of the population of the Republic of Bulgaria. The energy status of the cadets during complex tactical exercises was determined by comparing the studied energy expenditure and energy intake.**

Keywords*— *energy expenditure, energy intake, energy status, military personnel, macronutrients.

I. INTRODUCTION

The nutrition of military personnel of the Armed Forces of the Republic of Bulgaria is an important factor in maintaining the physical health of the personnel of the military formations and, respectively, conducting the combat training of the formations at a high level, which guarantees the fulfilment of the main tasks of the Armed Forces. The nutrition is always an essential part not only of the daily activity and training, but in real fighting circumstances also. This statement is proved by the fact that provision of food as an element of support and services for personnel is integral point of each Warning, Operational and Fragmentary order, issued in priority and in time of the battle. [1]

There are different formulations of the importance of nutrition for humans, but they are all related to the indisputable fact that without nutrition, regardless of whether it is rational, balanced, unbalanced, dietary (therapeutic), preventive or related to specific eating habits (vegetarianism, veganism or raw foodism), it is not possible to maintain the vital functions of the body. In the scientific space, there are numerous studies on human nutrition issues, various concepts of nutrition have been developed, specialized textbooks and collections have been issued, scientific articles and reports have been published, books have been proposed for the general public, but the theses that underlie them are scientifically based. Scientific evidence is what must be followed by nutritionists when compiling and balancing nutrition menus, taking into account the characteristics and factors affecting different groups of eaters or individual individuals. [2]

A. National physiological norms for nutrition of the population of the Republic of Bulgaria

Physiological nutritional norms are used in determining the national nutrition policy of the population, assessing individual nutritional intake and the nutritional intake of population groups, developing recommendations for healthy nutrition of individuals and population groups, planning and control of organized nutrition of population groups and include:

- Average energy needs - the estimated average values of energy dietary intake, minimizing the risk of exceeding and/or underestimating the levels of energy intake, balancing the respective energy expenditure of individuals from the population group,
- Recommended dietary intake of protein, carbohydrates, vitamins and minerals - an average daily level of dietary intake that provides the need for a particular nutrient for almost all (97.5%) healthy individuals in individual groups, differentiated by age, sex and physiological state (pregnancy and lactation). The recommended dietary intake is equal to the "average nutrient requirements" for the group plus two standard deviations,
- Adequate dietary intake of protein, total fat, fatty acids, total carbohydrates, dietary fibre, vitamins, minerals and electrolytes, when a recommended dietary intake cannot be determined -

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8508
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

recommended average daily intake of nutrients, representing the level of their average intake (median value) in a group of healthy individuals, determined on the basis of scientific research, which is assessed as adequate for all individuals in the group. It is used when average nutrient needs cannot be estimated and a recommended dietary intake can be determined on this basis,

- Adequate dietary intake of water,
- Upper Dietary Intake Limits for Vitamins, Minerals and Electrolytes - (ULNI) is the highest daily dietary intake level that is not associated with adverse health effects in nearly all individuals in a given population group. If intakes are higher than the ULNI, there is an increased risk of adverse health effects,
- Recommended dietary intake ranges for protein, total fat, fatty acids, total carbohydrates, and dietary fibre - the values associated with a low risk of chronic diseases provided adequate intake of essential amino acids, essential fatty acids, vitamins, and minerals.

Energy requirements are defined as average energy requirements, expressed in MJ and kcal per day for population groups differentiated by age and sex; at reference height and weight; estimated for different levels of physical activity and represent the average daily requirements for a period of at least one week.

The level of physical activity was also recorded, which was divided into the following levels:

- low activity lifestyle,
- moderately active lifestyle,
- active lifestyle,
- very active lifestyle. [3]

TABLE 1 RECOMMENDED/ADEQUATE INTAKE OF MACRONUTRIENTS

Age	**Recommended/Adequate Intake**					
	Protein (g/day)		***Fat (g/day)***		***Carbohydrates (g/day)***	
	м	***w***	***м***	***w***	***м***	***w***
19 - 29	58,1	46,5	72-126	56,2 – 98,3	367,5-490	286,7-382,2
30 - 59	59,7	49,8	72-126	56,2 - 98,3	367,5-490	286,7-382,2

II. MATERIALS AND METHODS

The study has been conducted among cadets from Vasil Levski National Military University, which was established 147 years ago as the first governmental institution in Bulgaria and has been functioning. Moreover, the organization has a primary role in the military educational system of the country, and it has been educating trainees for the regular and reserve component of the Bulgarian Armed Forces. [4]

The study has been conducted with cadets majoring in Motorized Infantry and Tank Troops, during their participation in a tactical exercise in summer conditions. A total of 13 (thirteen) cadets were studied, of which 11 (eleven) were men and 2 (two) were women. The average age of the cadets was 20 (twenty) years. The present study used the method of individual tabular timing, which accurately records the time spent on an activity. The tabular timing method accurately records the time spent on a given activity. The data obtained using energy consumption tables for different types of activities allow the determination of the individual's daily energy consumption. Initially, the time spent on the daily activities of an individual is measured, fixing their duration. A disadvantage of this method is the difficulty of predicting all activities throughout the day, and therefore the researchers believe that the error in this method is up to 15%. The advantage of the method is its general accessibility and simplicity. [5]

For the purposes of the study, an individual timekeeping table was developed for each cadet with certain fixation points for the individual activities and part of the day. They were given detailed instructions and the weight of each participant in the study was measured with an electronic scale with an accuracy of 0.1 kg. Before starting the study, preliminary training was carried out with the participating cadets on the features of filling out the individual timekeeping table. The types of loads related to the preparation of the cadets were recorded by measuring their duration in minutes. Based on the results of the five-day recording of the described types of physical and mental activity, the duration of each of them was determined for each student. The energy expenditure per unit of time (kcal/min) was determined using the indirect calorimetry method. The minute energy expenditure at rest was determined according to data from the World Health Organization, based on data on gender, age and weight. The value of the energy expenditure for one minute was multiplied by the duration of the specific physical activity during the day. The results obtained reflect the individual daily energy expenditure spent on each type of physical or mental activity. The obtained daily energy expenditure for the individual activities was summed to obtain the total value of the energy expenditure of each cadet during one day. To obtain the average value of the total daily energy expenditure, the corresponding individual values for men and women were summed and divided by the number of cadets studied. The following methods can be used to study energy consumption:

- record of the food consumed by the serviceman for a certain period - as a quantity of food products. The main energy suppliers are proteins, fats and carbohydrates (macronutrients). In order to determine the energy intake as kilocalories, the quantity of macronutrients consumed by the serviceman under study must be established. This can be established from the content of macroelements in the amount of food consumed. The content of macroelements can be obtained from the manufacturer or from the "Tables of the composition of Bulgarian food products". To

summarize these data, the tools of the Microsoft Excel software product are used,

- use of the prepared weekly menu for the servicemen's nutrition during their training. The data processing is in the same way described above.

III. RESULTS AND DISCUSSION

After the actual processing of the data from the study, the following results were obtained for the energy expenditure of the participants:

- for male trainees - average energy expenditure for the period - 4305 kcal,
- for female trainees - average energy expenditure for the period - 3460 kcal.

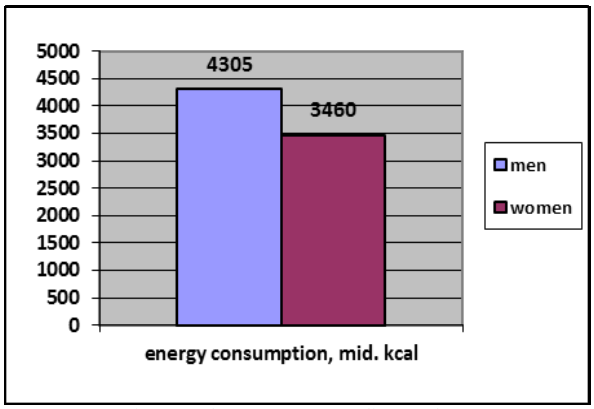


Fig. 1. Cadets' energy expenditure values.

Complex tactical training is characterized by prolonged movement over rough terrain and significantly less time for rest (sleep). The highest energy expenditure is shown by the cadets when moving over rough terrain with equipment and performing various tactical tasks on the terrain, as well as during physical exertion when building field camps.

In order to determine the energy intake, it is necessary to calculate the macronutrients consumed by the trainees during the study period. Macronutrients are nutrients that are necessary to maintain important functions of the human body. These include proteins, fats and carbohydrates.

Growth and development depend on the increase in the number of cells in the body. The main role in this important process is played by proteins. They participate in the construction and increase in the number of cells in the body. Proteins are made of amino acids, which are the main building blocks in the body. Carbohydrates provide most of the energy needed for the body to function. Fats are a concentrated form of energy and the form in which much of the body's energy reserves are stored. Fats are important for building cell membranes and are also involved in the absorption and use of some vitamins. [6]

The nutrition of the personnel of the BA is organized in accordance with the conditions and procedure for the provision of food, announced in a regulatory act of the Minister of Defence. The main regulatory document of 02.04.2015 is Regulation No. H-5 on the conditions, procedure and norms for providing free food and refreshments to military personnel and civilian employees of the Ministry of Defence, structures directly subordinate to the Minister of Defence and the Bulgarian Army and to cadets in higher military schools in peacetime. The regulation specifies energy and substance norms for balanced nutrition for one feeding day, where the values for macronutrient intake for field training are as follows: proteins - 150-170 grams, fats - 160-175 grams and carbohydrates - 510-560 grams.

For those categories of military personnel who work under conditions of great physical and nervous stress or are subject to the influence of adverse factors, an additional requirement is placed on the rations - to influence the normalization of the disturbed physiological state and contribute to increasing the body's resistance to the relevant adverse influences. [7]

The norms in Regulation No. 1 of January 22, 2018 on the physiological nutritional standards of the population in Bulgaria are the starting point for determining the composition of the daily food ration of military personnel, as no other modern specialized study is known for the Bulgarian Army. [8]

The regulation specifies recommended ranges for the intake of total protein, total fat, fatty acids and total carbohydrates as a relative share of the energy value of food (E %). The values for the age group from 19 to 65 years for the intake of these nutrients are as follows: total protein – 10-20 (E%), total fat – 20-35 (E%) and total carbohydrates – 45-60 (E%).

Proper nutrition ensures normal development of military personnel, promotes disease prevention, prolongs life, improves efficiency and creates conditions for adequate adaptation to the environment. An important stage in rationalizing decisions related to the intake of nutrients and energy by cadets is a study of the energy intake and nutritional status of students at the National Military University. [9]

The cadets were given food products for the period of field training, some of which were: pork shoulder, chicken leg, sausages, sausage, bacon, yellow cheese, cheese, butter, "Dobruja" bread, yogurt, eggs, beans, fresh cabbage, oranges, bananas, apples, waffles, croissants, various types of canned food products, vegetables, spices, etc.

After processing the data, the following results were obtained:

- during the training period, the cadets were provided with daily food with the following average macronutrient content - proteins - 203 grams, fats - 188 grams and carbohydrates - 637 grams,

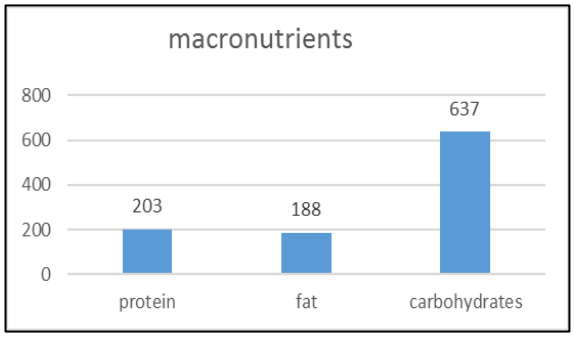


Fig. 2. Macronutrient content in grams.

- for the study period, macronutrients provided the cadets with the following average energy through the food they consumed - proteins - 832 kcal, fats - 1750 kcal, carbohydrates - 2611 kcal.

The largest energy carriers of food products provided daily for the trainees are - bread - 1775 kcal, meat - approximately 440 kcal, fish - approximately 308 kcal, sausages - approximately 300 kcal.

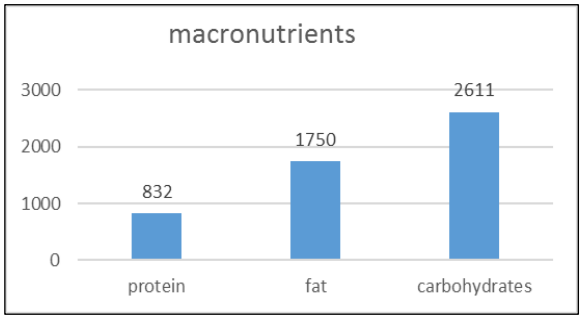


Fig. 3. Energy provided by macronutrients in kcal.

After comparing the results obtained for the intake of macronutrients by the cadets for the study period with the recommended intervals for the intake of total protein, total fat, fatty acids and total carbohydrates as a relative share of the energy value of food (E %) from Regulation No. 1 of January 22, 2018 on the physiological norms for nutrition of the population, the following is obtained: the total protein from the food provided to the cadets is 16.02% of the energy value, fats are 33.7%, and carbohydrates are 50.28%.

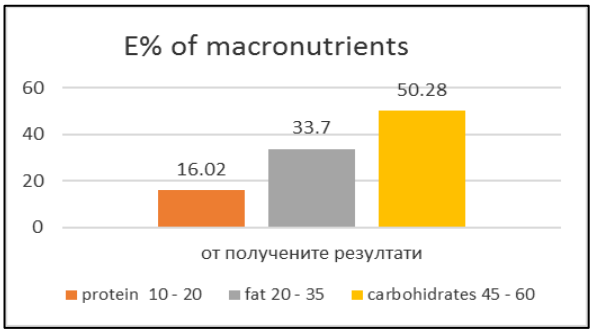


Fig. 4. It is a % ratio of macronutrients.

The results indicate that the intake of macronutrients largely corresponds to the physiological nutritional standards of the population in Bulgaria.

In percentage terms, macronutrients correspond to the physiological nutritional standards of the population, but when comparing them by intake in grams, things are as follows:

- for proteins - the recommended daily intake in grams for men is from 81.4 to 162.8, and for women it is from 63.7 to 127.4. The amount provided to the cadets is 203 grams,
- for fats - the recommended norms in grams are from 72 to 126 for men and from 56.2 to 98.3 - for women. The amount provided is 188 grams,
- for carbohydrates - the recommended intake in grams is from 367.5 to 490 for men and from 286.7 to 382.2 - for women. The quantity provided to the trainees is 637 grams.

TABLE 2 RECOMMENDED INTAKE AND MACRONUTRIENTS PROVIDED

	Protein	**Fat**	**Carbohydrate**
Recommended intake - men	81,4–162,8	72-126	367,5-490
Recommended intake - women	63,7-127,4	56,2-98,3	286,7-382,2
Macronutrients provided	203	188	637

After determining the energy expenditure of the studied group, we should determine the energy status.

During the tactical exercise, the servicemen were provided with food according to the appendices of the current nutrition regulation, which includes a basic application plus supplements required for various activities, such as exercises, increased energy expenditure, etc.

Based on the prepared menu-layout for the purposes of the exercise, the servicemen were provided with macronutrients, providing an average energy intake of 5184.25 kcal. per day per person.

After comparing the values, an imbalance is obtained between the energy intake of the servicemen and their energy expenditure. The average values show a difference of nearly 900 kcal in favour of energy intake in men and about 1700 kcal - in women.

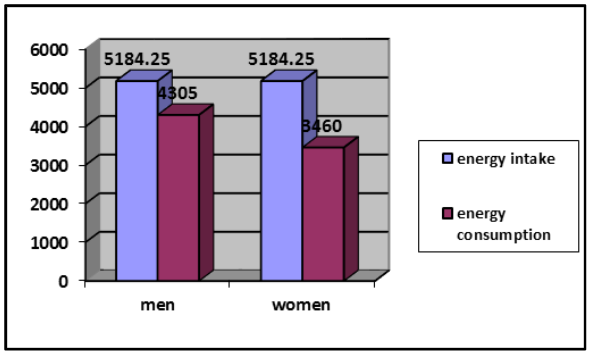


Fig. 5. Energy status.

IV. CONCLUSIONS

From the results obtained, it can be concluded that the nutrition of cadets during tactical exercises, in particular - the intake of macronutrients, is in extreme imbalance according to the nutritional standards of the population in Bulgaria. In this situation, it is advisable to develop new standards for the nutrition of cadets during tactical exercises, adequate to the needs.

From the results obtained for the energy status of military personnel during complex tactical exercises, it is again evident that their nutrition is in imbalance compared to their needs. Here too, it is necessary to propose a new set of food products that would ensure a balance in the nutrition of military personnel during complex tactical exercises.

V. ACKNOWLEDGMENTS

This report is in implementation of the National Scientific Program "Security and Defence", adopted by Decree of the Council of Ministers No. 731 of 21.10.2021.

REFERENCES

[1] N. Pavlovski, Planning of Combat Actions by the Company and Platoon According to the Formation Management Procedures (Troop Leading Procedures). Veliko Tarnovo, Vasil Levski National Military University Publishing Complex, 2024, pp. 48, 50, 51, 52, 53, 234. (ISBN 978-954-753-390-5 – soft cover, ISBN 978-954-753-391-2 – pdf and ISBN 978-954-753-392-9 – CD).

[2] P. Glushkov, " Experimental feeding of specific population groups", Monography, Veliko Turnovo, Bulgaria, 2019. [Eksperimentalno hranene na specifichni grupi ot naselenieto, Monografiq, Veliko Turnovo, Bulgariq, 2019].

[3] Naredba № 1/22.01.2018 y. for determining the physiological norms for nutrition of the population of the Republic of Bulgaria.[Naredba № 1/22.01.2018 g. za preporuchitelni fiziologichni normi za hranene na naselenieto na Republika Bulgariq].

[4] N. Pavlovski, Similarities and Differences in the Training of Cadets and Schoolman in Bulgaria at the End of the 19-th and the Beginning of the 20-th Century. Collection of Reports from the Jubilee Scientific Conference 140 Years of Military Education – Traditions and Perspectives of Vasil Levski National Military University. Veliko Tarnovo, 2019, pp. 39, 52. (ISBN 978-954-753-283-0).

[5] Определения суточных энергозатрат хронометражно-табличным методом: https://studopedia.ru/7_146662_opredeleniya-sutochnih-energozatrat-hronometrazhno-tablichnim-metodom.html [Accessed: Feb. 20, 2024].

[6] Д. Гьоргев, Здрава исхрана, Скопие, 2008.

[7] P. Glushkov,“ Food Supply and Nutrition in the Bulgarian Army“. Land Forces Academy Review Vol. XXII, No 4(88), 2017, pp. 213-218. DOI: 10.1515/raft-2017-0028.

[2] [8] P. Glushkov „Comparison of the normative basis for nutrition of the population with the nutritional standards for forces in preparation for expeditionary operations“, November, 2014.

[3] [Sravnenie na normativnata baza za hranene na naselenieto s normite za hranene za sili pri podgotovka za ekspedicionni operacii, Noemvri, 2014].

[9] N. Nichev, “Analysis of energy expenditure and energy intake of cadets from the Vasil Levski NMU”, Knowledge – internnational jurnal, vol.22.4, p. 1070, Serbia, march 2018.

[10] Naredba N - 5/02.04.2015 y. on the conditions, procedures and norms for providing free food and refreshments to military personnel and civilian employees of the Ministry of Defense, structures directly subordinate to the Minister of Defense and the Bulgarian Army and to cadets in higher military schools in peacetime. [Naredba N-5/02.04.2015 g. za usloviqta, reda i normite za osigurqvane na bezplatna hrana i obodrqvashti napitki v ministerstvoto na otbranata, strukturite na prqko podchinenie na ministura na otbranata i bulgarskata armiq].

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference .2025. Volume V, 141-148

Security in Legal Education: Challenges and Solutions in the Modern World

Inga Kudeikina
Faculty of Social Sciences
Riga Stradiņš University
Riga, Latvia
inga.kudeikina@rsu.lv

Sandra Kaija
Faculty of Social Sciences
Riga Stradiņš University
Riga, Latvia
sandra.kaija@rsu.lv

Ivans Jānis Mihailovs
Faculty of Social Sciences
Riga Stradiņš University
Latvian Academy of Culture
Riga, Latvia
ivans.mihailovs@rsu.lv

Lidija Juļa
Faculty of Social Sciences
Riga Stradiņš University
Riga, Latvia
lidija.jula@rsu.lv

Vitālijs Rakstiņš
Faculty of Social Sciences
Riga Stradiņš University
Riga, Latvia
vitalijs.rakstins@rsu.lv

***Abstract*—Legal education is an essential foundation for the sustainability and development of society, ensuring democracy and security by preparing future lawyers, including judges. In an era of rapid digitalization, security issues in legal education are becoming increasingly relevant. Problems such as access to confidential documents, insufficient knowledge of digital security risks, and the lack of protection mechanisms pose significant threats to students, faculty, and lawyers. Addressing these issues is essential to maintain trust in the legal system and ensure the integrity of legal education. The aim of this study is to analyze security aspects in legal education, focusing on the need to improve students' understanding of legal and practical security issues. The study explores how cybersecurity training can be integrated into legal education so that future lawyers acquire the necessary skills to responsibly handle sensitive information in a secure digital environment. The study uses a qualitative research approach that includes a review of the legal framework, academic literature and case studies on cybersecurity challenges in legal education. Comparative analysis is used to examine best practices across jurisdictions regarding security measures in legal studies. In addition, expert opinions from legal professionals and educators are taken into account to assess the effectiveness of current approaches and identify areas for improvement. The results highlight the need to integrate cybersecurity courses into legal education curricula and improve regulatory frameworks to address digital security risks. A more comprehensive approach to legal education that includes practical cybersecurity training would improve students' ability to navigate ethical and professional challenges in the digital age. Implementing these measures would not only reduce cybersecurity risks but would also better prepare law students for their professional responsibilities by ensuring their competence in protecting sensitive legal information.**

Keywords - cybersecurity, data protection, legal education.

I. INTRODUCTION

Legal education is an essential foundation for the sustainability and development of society, ensuring democracy, security, and the rule of law, as it prepares future lawyers, including judges, security institution employees, and other legal specialists [1], [2]. According to the explanation given in the National Encyclopedia, legal education is a set of systematized knowledge in legal sciences; the system of acquiring this knowledge in educational institutions, the process of legal education, the theory, practice, and didactics of teaching legal sciences, legal education, as well as continuous professional development [3]. Therefore, in addition to academic challenges, it is important to pay attention to security aspects that affect students, teaching staff, and practicing lawyers (also in accordance with the Latvian Cybersecurity Strategy for 2023–2026 [4]). In today's rapidly changing world, where information and communication play a significant role, security issues in legal education are becoming increasingly relevant. For example, access to confidential documents, insufficient knowledge of digital security risks, and a lack of protection mechanisms create significant problems that can threaten the security of both students and institutions. Higher education institutions should pay increasing attention to these issues by improving studies and integrating relevant study courses into the study process [5], [6]. Also, the use of AI in education offers unique opportunities in legal education. AI

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8472
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

systems, with their vast databases and analytical capabilities, can present students with complex problems and scenarios that require more than just rote memorization or basic understanding. These systems can challenge students to use higher-order thinking skills, such as analysis, synthesis, and evaluation, to navigate through these problems [7], [8]. To ensure the effective implementation of AI, cybersecurity policies, legal education must include specialized knowledge of cybersecurity laws and their practical application [9]. Another important concern is the readiness of students to work with digital legal resources and their ability to mitigate potential security risks associated with using online databases and other digital tools [5]. This article will analyze certain security aspects in legal education that affect the improvement of the study process, ensuring that future lawyers develop an understanding of the legal and practical aspects of security during their studies and acquire the necessary cybersecurity skills and abilities to work with sensitive information in a secure digital environment.

II. Materials and Methods

The purpose of this work is to analyze cybersecurity problems in legal education and offer effective solutions for the protection of confidentiality and sensitive data to improve students' readiness to work with digital legal resources and prevent possible security risks. To achieve this goal, the study will employ the analysis of legal acts and legal doctrine, including academic research and expert opinions on security issues in the education of future legal professionals.

III. Results and Discussion

A. The Importance of Legal Education in Public Safety and Sustainable Development

Legal education is one of the cornerstones of sustainable development and security of society, ensuring that members of society understand their rights and obligations, promoting the rule of law, and strengthening state power. When evaluating the importance of legal education in the context of state power functions, in Latvia, the Ministry of Justice, namely the executive branch, is responsible for the state unified lawyer exam, which is presumed to be one of the guarantees of legal education quality. In carrying out its duty, the executive branch also ensures the functioning of the judiciary. Although the existence of legal education provides opportunities to work in various professions and offers broad career opportunities, the requirement to obtain higher education and professional qualification as a lawyer is mandatory for persons in the judicial system – judges, prosecutors, sworn advocates, sworn notaries, and sworn bailiffs. In the judicial system, where justice is administered and important decisions are made that affect people's lives, there are strict requirements regarding professional training, ensuring both competence and responsibility in performing assigned duties. This requirement not only guarantees that the judicial system will function effectively but also strengthens public trust in the rule of law and its institutions, since only qualified persons can ensure objective and fair judicial work. This is especially important in the context of the separation of powers, as only qualified and independent lawyers can ensure that judicial decisions are made objectively, in compliance with all legal principles, and are effectively executed, which, in turn, promotes public trust in the rule of law. In connection with these important aspects, especially regarding judges as guarantors of the right to a fair trial, it has been rightly stated in the scientific literature that public trust in the judicial system as the basis of public welfare depends on judges [10].

Legal education is an essential basis for obtaining a position in the judicial system, as it provides the necessary knowledge, skills and competences that are important for fulfilling a responsible position in the judicial system. The work of these persons is related to the interpretation and application of laws in specific cases, as well as to observing justice and the rule of law, which requires both theoretical knowledge and practical skills. However, legal education is an important, but not the only prerequisite for obtaining, for example, the position of a judge. It is the first step towards professional activity in the judicial system. The state imposes a number of requirements on applicants for the position of a judge, namely, it determines not only the education requirement, but also, for example, the citizenship, age, professional experience requirement.

Historically, judges could be “just a decent person” (without any educational qualifications). Historical sources indicate that the situation in Europe changed in the 18th century, when professionals, educated lawyers, became judges, one of the reasons being that legal norms were codified [11]. In addition, previously, work in the relevant field had to start from office and then, while already working, one had to study the relevant norms. However, today, the legislator has provided for the possibility of immediately becoming a judge of a regional court or the Supreme Court with education and professional experience, theoretically without working a single day in the judicial system. Currently, the educational qualification plays a significant role in the work of a judge. First of all, so that a person, upon becoming a judge, can immediately begin to perform the duties of a judge, and also to judge qualitatively. You, so that a judge can constantly improve his or her qualifications. Here it is necessary to recall what was mentioned at the beginning of the chapter, that legal education is also the improvement of qualifications / professional competence. Continuous improvement of qualifications is an essential component of any profession. It is also essential in the selection of candidates for the position of judge. Because not only the formal criteria – the presence/absence of higher education and professional qualifications as a lawyer, as well as the existence of a master's or doctoral degree – are important, but also the ability and competence to improve one's qualifications.

Here it can be argued: if ensuring the training of appropriately qualified lawyers is the task of the executive branch, then the task of the judicial system itself is to create a supportive, development-oriented environment in which each judge could improve their skills and qualifications.

The quality of legal education directly affects the competence not only of judges, but also of lawyers, prosecutors and other judicial system employees, which in turn

determines how effectively rights and justice are ensured in society.

Despite acquiring theoretical knowledge, legal education graduates face difficulties in applying practical skills. Legal study programs often do not sufficiently emphasize the development of critical thinking problem-solving and practical skills, which are essential for effective legal practice and ensuring public safety.

Critical thinking plays a vital role in legal education. The scientific literature indicates that applied to law, critical thinking is the ability: 1) to evaluate a legally relevant object from a specific legal-doctrinal, legal-empirical or legal-theoretical normative framework, using relevant (legal and other) sources of information; 2) A legally relevant object can be: a) the existing law (legislation, court decisions, treaties and so on), b) the legal and political system (including, for instance, the legislature, the administration and the judiciary), c) current legal opinions or theories about the law and the legal and political system (such as legal positivism or ELS) or d) actions from legal and political authorities (such as the police) or citizens; 3) to express one's own opinion about it which deviates from the mainstream understanding; 4) and to substantiate this opinion with good arguments based on standards derived from this specific framework [12].

For example, on 7 November 2019, the Constitutional Court adopted a judgment in case No. 2018-25-01, which assessed the compliance of Article 50.4 of the Latvian Penal Code with Article 91 of the Constitution. This article established different regimes for serving sentences for men and women serving sentences of deprivation of liberty in a closed prison. The Constitutional Court concluded that such a difference was not objectively and reasonably justified, thus violating the principle of equality enshrined in Article 91 of the Constitution. Consequently, the Constitutional Court found this legal regulation to be inconsistent with Article 91 of the Constitution. [13].

When analyzing this judgment, the following methodology can be used: 1) The judgment is assessed considering Article 91 of the Constitution, which establishes the principle of equality – "all persons are equal before the law". This principle is essential to ensure that discriminatory differences are not created in the application and results of national legal acts based on unnecessary criteria, such as gender. The judgment of the Court also analyzes the Latvian Penal Code, which establishes different sentencing regimes for men and women. The Court recognizes that such regulation, which establishes discrimination based on gender, is contrary to Article 91 of the Constitution, because gender differences are not objectively and reasonably justified. Thus, within the framework of the legal analysis, it is recognized that it is not justified by the principle of non-discrimination and balanced legal values. 2) The object of the judgment is the existing law – the Latvian Penal Code – which regulates sentencing regimes. The task of the court was to assess the compliance of this regulatory act with Article 91 of the Constitution, considering that the right to equality is one of the pillars of fundamental rights. The court's conclusion on the need to prevent gender discrimination in the service of punishment is based on the interpretation of this norm. 3) In this case, the court takes a critical attitude towards the norms of the law that considered gender differences to be justified, indicating that the regulatory framework must be changed. The court indicates that gender differences cannot be justified by the need to create different conditions in prisons, and considers them to be unfounded and unnecessary, since it directly violates the individual's right to equality. 4) The court rightly indicates that gender discrimination in the regime of execution of punishment is contrary to the principles of the Constitution. The argumentation is based on the fundamental principles of the legal system, namely, the principles of equality, justice and respect for human rights. The court implemented a critical thinking approach to social justice and the prevention of discrimination, which allowed it to identify an unnecessary gender difference in the regulation.

This judgment is an example of how a court is able to express an independent and critical opinion, assessing the inequality of existing norms and proposing changes that have a beneficial effect on human rights and the rule of law in the state.

The aim of legal education is not only to provide theoretical knowledge of legal norms, but also to develop the ability to critically analyze and understand laws and the practice of their application. Critical thinking skills are an essential element in legal education, as they allow students not only to understand and master the laws, but also to analyze, evaluate and challenge the existing legal framework and make legal decisions that are objective and justified. A lawyer with high critical thinking skills is able to ask important questions about the existing legal system and its effectiveness.

Critical thinking encourages the search for alternative approaches to specific problems and issues. It is not limited to the application of existing laws, but also allows students to seek new, innovative methods of solving legal problems or interpreting laws, which is necessary, for example, in legal research or case law.

We must not forget about artificial intelligence either. The use of AI in education offers unique opportunities to cultivate critical thinking. AI systems, with their vast databases and analytical capabilities, can present students with complex problems and scenarios that require more than just rote memorization or basic understanding. These systems can challenge students to use higher-order thinking skills, such as analysis, synthesis, and evaluation, to navigate through these problems [8].

In addition, critical thinking helps to create a responsible attitude towards the use and application of law, promotes the development of legal culture, which undoubtedly strengthens public safety.

Critical thinking skills are also vital in cybersecurity to evaluate technologies, address security challenges, and make informed and long-term decisions about organizational security. It helps to measure risks, predict potential

threats, and respond effectively to cybersecurity incidents, while adhering to legal and ethical standards. Thus, critical thinking in cybersecurity becomes an important tool to ensure effective and sustainable protection against cyber threats.

The legal system is changing, and only those lawyers who are able to think critically can actively participate in its improvement, ensuring justice and efficiency. Thus, universities today must strive to provide students with the intellectual studies, critical thinking skills necessary for high-level leaders in a complex future society.

B. The role of legal education in strengthening cybersecurity and sustainable societal development

In today's digital age, legal education plays a crucial role not only in promoting public safety and sustainable development but also in strengthening cybersecurity. An effective legal education ensures that future and current lawyers, judges, and other legal professionals are well-versed in existing regulatory frameworks and policy planning documents while also being equipped to address new challenges posed by rapid technological advancements.

One of the key issues is how legal education can prepare specialists to effectively prevent cyber threats and respond to cybersecurity incidents. How can we ensure that lawyers are not only familiar with legal regulations but also capable of applying this knowledge in practice by developing and implementing effective security measures? [9]. Another critical concern is the readiness of students to work with digital legal resources and their ability to mitigate potential security risks associated with using online databases and other digital tools [5].

Cybersecurity legislation and policy documents establish the legal framework necessary to protect critical infrastructure, personal data, and other sensitive information. The European Union's Directive on security of network and information systems (NIS Directive) [14] and the General Data Protection Regulation (GDPR) are prime examples of the growing importance of cybersecurity legislation.

To ensure the effective implementation of cybersecurity policies, legal education must include specialized knowledge of cybersecurity laws and their practical application. Lawyers specializing in cybersecurity can make a significant impact in both the public and private sectors, helping to create a secure and well-regulated digital environment [15].

C. Cybersecurity in education: challenges and solutions

Cybersecurity has become one of the most critical areas affecting all aspects of life, including education. Higher education institutions increasingly rely on e-learning platforms, which, while offering flexibility and accessibility, also introduce new risks related to the security of sensitive data and academic content. The main threats include unauthorized access to study materials, personal data leaks, and ransomware attacks, all of which can disrupt academic processes and have serious consequences for both students and faculty.

Recognizing these challenges, Regulation 2021/887 of the European Parliament and of the Council, adopted on 21 May 2021, established the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC). The primary objective of the ECCC is to promote research, innovation, and implementation in the field of cybersecurity by supporting the European Union (EU) Cybersecurity Competence Community. This community consists of public authorities and private sector participants working together under the framework defined by the Regulation. In Latvia, the National Cybersecurity Center has been actively addressing cybersecurity risks in the education sector, particularly concerning the use of e-learning platforms and university study resources [15].

The academic environment has become an attractive target for cyber attackers. Various digital platforms used in the study process store both academic and personal data, making secure data management crucial to prevent breaches and unauthorized access. Data leaks can have severe consequences for students and educational institutions alike. For example, at the end of 2024, a significant data breach occurred in Latvia's Unified Local Government Information System, affecting residents of 42 municipalities (excluding Riga). The leaked data included names, surnames, personal identification numbers, declared addresses, and even metadata from municipal employee documents. This incident is considered the largest known data breach in Latvia [16].

Such security breaches pose significant risks, as the exposed information can be exploited for fraudulent activities, including phishing scams and identity theft. The scientific literature highlights that “academic institutions are particularly vulnerable to cyber threats due to their valuable intellectual property, sensitive personal data, and research data.” Cyberattacks targeting universities range from phishing schemes and ransomware attacks to sophisticated attempts to steal research data, ultimately threatening the integrity of research and financial stability [6].

Latvian universities are increasingly facing cyberattacks that involve both data leaks and damage to information systems. These incidents not only disrupt the learning process but also create dissatisfaction among students and faculty, undermining trust in digital education. The CERT.LV activity report for the third quarter of 2024 revealed a 267% increase in cyber threats, highlighting a surge in attacks on virtual environments. Analysis indicates that many of these attacks are politically and commercially motivated, with support from Russia and China, though the majority have been successfully neutralized [17]. This alarming trend underscores the urgent need for enhanced cybersecurity measures and effective cooperation between academic institutions and security experts to ensure a safe and stable learning environment.

The rapid advancement of artificial intelligence (AI) technologies presents new challenges in education. AI can be exploited to conduct automated phishing campaigns, generate fake academic resources, and simulate cyber threats, misleading students and faculty and endangering academic integrity. Additionally, deep fake technology

enables the creation of falsified video and audio materials, which could compromise the reputation of educational institutions or spread disinformation. Disinformation campaigns aim to destabilize academic institutions and erode public trust in the education system [6]. These emerging threats highlight the necessity of a comprehensive cybersecurity approach in education, combining technological solutions with the development of critical thinking skills.

Cybersecurity has gained increasing importance at the national level as security threats continue to evolve. To strengthen national cybersecurity, the Cabinet of Ministers approved the Latvian Cybersecurity Strategy for 2023–2026 on 14 March 2023. This strategy outlines key policy directions and identifies future threats, focusing not only on strengthening technological protection but also on fostering international cooperation and enhancing public awareness of cybersecurity issues. The education sector plays a crucial role in implementing cybersecurity policies and developing protection systems [4].

Latvia has been actively developing cybersecurity policies in the education sector, involving various organizations. The Ministry of Defence, in collaboration with CERT.LV, the University of Latvia, and the National Guard Cyber Defence Unit, annually organizes a cybersecurity challenge for young people to develop their knowledge and skills in this field [18]. Additionally, Riga Technical University (RTU) has launched a two-year cybersecurity education project aimed at preparing students and professionals for careers in cybersecurity [19]. Similarly, the professional master's study programme "Cybersecurity Engineering" at Vidzeme University of Applied Sciences provides in-depth knowledge and essential skills for security testers and other specialists in this field [20].

D. Cybersecurity risks in legal education

Modern legal education increasingly relies on digital technologies and information systems, particularly in distance learning and online assessments. However, this growing dependence on digital tools also exposes legal education to various cybersecurity risks, which can be categorized as follows:

1) Disruptions to the Study and Research Process Cyberattacks targeting the websites and databases of educational institutions, as well as online study and examination tools, can severely disrupt legal education. Unauthorized access or remote manipulation of information systems may lead to the complete suspension of distance learning, compromise the objectivity of assessments, or interfere with automated grading algorithms. Additionally, the uncontrolled advancement of disruptive technologies, particularly artificial intelligence solutions, heightens the risk of their malicious use [21].

2) Threats to Data Availability and Integrity Cyberattacks can compromise data availability—for instance, by encrypting critical data, rendering cloud-hosted information inaccessible, or even deleting data entirely [10]. Moreover, attackers can alter original files without authorization, undermining data integrity. Such risks pose significant challenges to the continuity of legal education.

3) Reputational and Confidentiality Risks Data breaches that expose sensitive information to unauthorized third parties can damage the reputation of educational institutions. These risks may involve data leaks, industrial cyber espionage, and intellectual property theft, all of which can have long-term consequences for both students and faculty.

4) Cybercrime Risks Security vulnerabilities in the digital environment also make legal education institutions potential targets for cyber fraud and other cybercrime activities [22].

While cybersecurity risks cannot be entirely eliminated, legal education institutions can implement a range of measures to ensure minimum cybersecurity standards, mitigate system vulnerabilities, and develop business continuity plans. However, there are currently no external regulations that require legal education institutions to adopt mandatory cybersecurity protection measures. It is also important to note that most cybersecurity measures do not require significant financial investments [23].

E. Regulatory acts and policy planning documents for strengthening cybersecurity in legal education

Technological developments and new risks, as well as several current geopolitical events, have contributed to the relatively rapid development of cybersecurity regulation, especially in the last five years. Political scientists Evija Djatkoviča and Māris Andžāns have published an overview of significant regulatory enactments and policy planning documents in this area until 2021 [24]. Therefore, this part of the article focuses on the most recent documents, as well as those aspects that affect legal education.

On 1 September 2024, the National Cybersecurity Law entered into force, defining cybersecurity in Article 1 as "activities that meet the definition set out in Article 2(1) of Regulation 2019/881" [25], i.e. "'cybersecurity' means activities that must be carried out to protect network and information systems, their users and other persons affected by cyber threats" [26].

The Latvian Cybersecurity Strategy for 2023-2026 envisages identifying the current training opportunities for cybersecurity specialists and identifying the needs of future cybersecurity specialist education programs, accordingly developing a plan for the training of cybersecurity specialists, starting from secondary vocational education to second-level higher education. The document also recognizes that "the introduction of professional standards, which need to be developed in accordance with existing international standards, is also essential", as well as promoting the rule of law in cyberspace and reducing cybercrime [4].

This directly resonates with the goal set out in the Digital Transformation Guidelines for 2021–2027: "A high level of digital security and trust in Latvia's digital space is ensured by the implementation of a modern cybersecurity policy, intensive use of reliable electronic identification

and other trust services, as well as effective protection of personal data and other rights in the digital environment," which actually requires every citizen to master various digital technologies and develop digital skills, because "the individual's opportunities to get educated, compete in the labor market, and fully participate in social processes depend on them" [27].

The provisions of these documents create the need to implement significant changes in education, including legal education, by improving studies and integrating relevant study courses into the study process in order to reduce the threat to both students themselves and various institutions, as well as develop the competence to identify and assess specific cyber problem cases.

It should be noted that critical thinking, safety and cybersecurity issues are already an essential part of the curriculum developed in the competency-based approach at the primary and secondary levels of education, as a cross-cutting skill in developing digital literacy - the learner effectively uses digital technologies for various purposes, analyzes the benefits and risks of digital communication, critically analyzes the reliability of information in the media; when creating their own content, they observe privacy, ethical and legal conditions; evaluate, adapt to their needs and follow healthy and safe technology usage habits [28].

In primary education, the learner must be able to analyze and assess the impact of technology on mental and physical health, society and the environment. To observe healthy and safe habits of using technology, justify their necessity. To construct, control and manage their digital identity [29]. In secondary education, in order to implement diverse plans, the learner must be able to purposefully choose or adapt and effectively use appropriate digital technologies, analyze the benefits and risks of digital communication, behave responsibly and communicate in the digital environment in accordance with their own and others' interests [28], [30].

The latest national professional higher education standard also states that the strategic goals of the first and second cycle professional higher education study programs are to ensure that graduates are able to responsibly and safely choose and use information technologies for the performance of work duties, research and lifelong learning, as well as for the acquisition, creation and sharing of digital content [30].

These goals also directly correspond to the challenges posed by the use of artificial intelligence, stipulating that "a data analytics course should be integrated into most programs in higher education" [7]. In turn, the information report "Strategic Roadmap for the Digital Decade for Latvia by 2030" states: "In the 2023 Digital Decade Report on Latvia, the European Commission has recommended accelerating efforts in the field of digital skills. Namely, Latvia is encouraged to continue implementing measures to integrate digital solutions into the education system throughout the entire education cycle, integrating them into all subjects" [31].

Combining the importance of legal education in public safety and sustainable development with regulatory enactments and policy planning documents to strengthen cybersecurity, it can be concluded that legal education is indispensable in modern society. Its main challenge is to ensure that lawyers are prepared to identify and prevent cyber threats, promoting a safe and sustainable digital environment.

IV. Conclusion

In legal science study programs, student training usually focuses on the analysis and interpretation of legal acts, developing practical skills for working with various legal sources, but cybersecurity issues, including those set forth in the legal profession standard, may currently often not be sufficiently addressed during the study program.

In the legal education process, cybersecurity and the protection of sensitive data are of fundamental importance, as students regularly work with confidential information, law enforcement and court practice materials, and legal databases during both academic studies and professional practice. However, there are several significant challenges in the current system:

Firstly, a lack of education on cybersecurity among students could pose a significant risk of data breaches. To mitigate this risk, it is imperative that law students have access to supplementary learning materials and training in secure computing and the protection of digital information. This will serve to reduce the likelihood of accidental or unintentional data leakage.
Second, digital resources used in legal databases and distance learning may not be adequately protected against potential cyber-attacks. Access to electronic court systems could be vulnerable if secure authentication mechanisms are not used, but this depends on the specific safeguards in place.
Thirdly, breaches of confidentiality may occur during student placements, particularly where there are no clear guidelines for the secure storage and transmission of sensitive documents. Personal email accounts, insecure cloud storage and poorly chosen passwords are sometimes used, which can increase the risk.
Fourthly, security vulnerabilities in students' personal devices could pose a risk to the protection of sensitive data. This can happen if students use poorly secured devices that may not have the necessary encryption tools and cybersecurity solutions.

Fifth, the specificity of legal education is associated with good skills in using information and communication technologies, as, for example, the national unified professional qualification exam for lawyers is taken in an electronic environment, as well as with several challenges of using various technologies and artificial intelligence in legal studies and research (which simultaneously raises several issues related to academic integrity).

Furthermore, although universities already offer various security solutions, current cybersecurity policies are often not sufficiently strict or effective to prevent potential threats.

To ensure confidentiality and the protection of sensitive legal data in legal education, specific measures are needed in two main areas: practical measures and the inclusion of requirements in legislation.

Although cybersecurity issues in legal education are not yet sufficiently developed, it is clear that they are becoming increasingly relevant as digitalization continues to affect the study process. To ensure that law students are prepared to work with sensitive data and understand security risks, universities need to take targeted measures to improve cybersecurity.

By introducing specialized training, improving e-study security mechanisms, and developing stricter confidentiality and quality guidelines, it is possible to achieve that the legal education environment becomes safer and more responsive to today's digital and security challenges.

Students who learn to use secure digital tools and understand the principles of data protection will be better prepared to work in courts, law firms, law enforcement agencies, etc. in the future, promoting trust and security in general.

Proposals for practical measures: 1) Integrating cybersecurity training into the study process – include cybersecurity and data protection courses as mandatory study content in law study programs; organize practical seminars and training on secure processing of sensitive data using real cases from legal practice; provide students with information resources on cybersecurity, including guidelines on secure password use, encryption technologies and secure data storage. 2) Strengthen the protection of sensitive data during student internships – set clear guidelines for students' handling of confidential data, for example, prohibiting storing it on personal smart devices/computers or transferring it using insecure emails; ensure that documents used during student internships are encrypted and accessible only to authorized persons; universities should work more closely with internship sites (courts, law firms, etc.) to ensure compliance with confidentiality policies and necessary training for students and internship sites; develop guidelines for secure device use, emphasizing the need for strong passwords, secure cloud storage, and regular system updates; promote student awareness of secure online communication using encrypted emails and file transfer tools.

Proposals for improving the regulatory framework: 1) Internal regulations of higher education institutions on data security – develop and implement a unified cybersecurity policy that regulates student access, document storage and information protection; clarify liability for violations of sensitive data processing and provide for liability for confidentiality violations in the study process. 2) Amendments to legal acts to strengthen cybersecurity in legal education – develop guidelines for universities on minimum data protection standards based on GDPR requirements; review the regulation of access to legal databases, ensuring that only registered users with appropriate rights can access sensitive legal materials; regulate the security of digital exams and distance learning, stipulating that secure authentication and monitoring mechanisms are used during exams; improve the standard of the legal profession by supplementing the acquisition of content related to (cyber)security and data protection during legal studies. 3) Cooperation between the judicial system and universities on cybersecurity issues – promote cooperation between universities and judicial institutions in the development of cybersecurity policy to provide students with practical knowledge of data protection in the judicial system; cooperate with IT security specialists to adapt study processes to the latest technological requirements; prepare recommendations for the Ministry of Justice for the implementation of digital security measures in legal education.

Overall, ensuring the security of sensitive data in legal education requires both a practical approach to student education and improving the use of technology, as well as the development of legislation that sets stricter security and data protection standards in higher education. The implementation of these measures would not only help reduce cybersecurity risks in legal education, but would also prepare students for professional activities in the digital age, where mitigating and protecting against cybersecurity risks is a key issue of professional ethics and responsibility.

REFERENCES

[1] I. Kudeikina and S. Kaija, "Problems relating to judicial selection in the context of sustainable development of society," European Journal of Sustainable Development, vol. 11, no. 4, 2022.

[2] J. Smith, Legal Education and Societal Security: Building a Sustainable Future. Cambridge University Press, 2021.

[3] D. Apse, "Juridiskā izglītība." Available: https://enciklopedija.lv/skirklis/2570-juridisk%C4%81-izgl%C4%ABt%C4%ABba. [Accessed: Feb. 10, 2025].

[4] "Latvijas kiberdrošības stratēģija 2023.–2026. gadam." Available: https://www.mod.gov.lv/sites/mod/files/document/Latvijas%20kiberdro%C5%A1%C4%ABbas%20strat%C4%93%C4%A3ija%202023.-2026.gadam_.pdf. [Accessed: Feb. 15, 2025].

[5] T. Brown, "Cybersecurity measures in higher education," Journal of IT Security, vol. 12, no. 3, pp. 45-58, 2020.

[6] Handbook for Academic and Scientific Institutions Improve Risk Management and Institutional Resilience in the Face of Security Threats. Rīga, RSU, 2024.

[7] "Informatīvais ziņojums 'Par mākslīgā intelekta risinājumu attīstību.'" Available: https://likumi.lv/ta/id/342405-par-maksliga-intelekta-risinajumu-attistibu. [Accessed: Feb. 15, 2025].

[8] Y. Walter, "Embracing the future of artificial intelligence in the classroom: The relevance of AI literacy, prompt engineering, and critical thinking in modern education," International Journal of Educational Technology in Higher Education, vol. 21, no. 15, 2024.

[9] L. Johnson and K. Miller, Cybersecurity Law and Policy: An Essential Guide. Routledge, 2020.

[10] J. Doe, "WannaCry ransomware impact on institutions," Cybersecurity Journal, vol. 5, no. 2, pp. 33-40, 2018. [Accessed: Feb. 10, 2025].

[11] S. Osipova, "Tiesneša ētika. Komunikācijas ētikas dimensija: nodotās informācijas skaidrība." Available: https://www.satv.tiesa.gov.lv/runas-un-raksti/tiesnesa-etika-komunikacijas-etikas-dimensija-nodotas-informacijas-skaidriba/#_ftn2. [Accessed: Feb. 10, 2025].

[12] B. van Klink, "Critical thinking in academic legal education," LaM, Aug. 2023.

[13] Satversmes tiesas spriedums par Latvijas Sodu izpildes kodeksa 50.4 panta atbilstību Latvijas Republikas Satversmes 91.

pantam. Available: https://www.satv.tiesa.gov.lv/cases/. [Accessed: Feb. 15, 2025].

[14] European Commission, "Directive on security of network and information systems (NIS Directive)." Available: https://ec.europa.eu. [Accessed: Feb. 10, 2025].

[15] Aizsardzības ministrija. Available: https://www.mod.gov.lv/lv/zinas/uzsakts-darbs-pie-kiberdrosibas-izglitibas-cela-kartes-izstrades. [Accessed: Feb. 15, 2025].

[16] K. Kairis, "Tehniska brāķa dēļ noplūst pašvaldību darbinieku un iedzīvotāju dati." Available: https://www.lsm.lv/raksts/zinas/latvija/13.11.2024-tehniska-braka-del-noplust-pasvaldibu-darbinieku-un-iedzivotajudati.a576336/. [Accessed: Feb. 15, 2025].

[17] CERT.LV, "Darbības pārskats, 3. ceturksnis, 2024." Available: https://cert.lv/lv/2024/11/cert-lv-darbibas-parskats-par-2024-gada-3-ceturksni. [Accessed: Feb. 15, 2025].

[18] "Aicinām piedalīties Latvijas kiberdrošības izaicinājumā 2025." Available: https://www.visc.gov.lv/lv/jaunums/aicinam-piedalities-latvijas-kiberdrosibas-izaicinajuma-2025. [Accessed: Feb. 15, 2025].

[19] RTU, "RTU ar partneriem kiberdrošībā izglītos studentus." Available: https://lvportals.lv/dienaskartiba/370581. [Accessed: Feb. 15, 2025].

[20] "Kiberdrošības inženierija." Available: https://va.lv/studijas/magistrs/kiberdrosibas-inzenierija. [Accessed: Feb. 12, 2025].

[21] A. Smith and B. Jones, "Artificial intelligence and data security risks," AI & Law Review, vol. 9, no. 4, pp. 22-35, 2020.

[22] L. Johnson and K. Lee, "Phishing attacks in digital education," International Journal of Cybersecurity, vol. 14, no. 1, pp. 67-79, 2022.

[23] A. Brown, Digital Legal Resources and Cybersecurity Challenges in Education. Oxford University Press, 2022.

[24] E. Djatkoviča and M. Andžāns, "Latvia: Entangled system-in-progress amidst terrorism, Russia and cyberthreats," in M. Andžāns, A. Sprūds, and U. Sverdrup, Eds., Critical Infrastructure in the Baltic States and Norway: Strategies and Practices of Protection and Communication. Latvian Institute of International Affairs, 2021.

[25] ["Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par ENISA ... (Kiberdrošības akts)." Available: https://eur-lex.europa.eu/eli/reg/2019/881/oj/?locale=LV. [Accessed: Feb. 15, 2025].

[26] Nacionālās kiberdrošības likums. Available: https://likumi.lv/ta/id/353390. [Accessed: Feb. 15, 2025].

[27] "Digitālās transformācijas pamatnostādnes 2021.-2027. gadam." Available: https://www.varam.gov.lv/sites/varam/files/content/files/digitalas-transformacijas-pamatnostadnes-_2021-27.pdf. [Accessed: Feb. 15, 2025].

[28] Ministru kabineta 2019. gada 3. septembra noteikumi Nr.416. “Noteikumi par valsts vispārējās vidējās izglītības standartu un vispārējās vidējās izglītības programmu paraugiem”. Available: https://likumi.lv/ta/id/309597. [Accessed: Feb. 15, 2025].

[29] Ministru kabineta 2018. gada 27. novembra noteikumi Nr. 747. “Noteikumi par valsts pamatizglītības standartu un pamatizglītības programmu paraugiem”. Available: https://likumi.lv/ta/id/303768. [Accessed: Feb. 15, 2025].

[30] Ministru kabineta 2023. gada 13. jūnija noteikumi Nr. 305. “Noteikumi par valsts profesionālās augstākās izglītības standartu”. Available: https://likumi.lv/ta/id/342818-noteikumi-par-valsts-profesionalas-augstakas-izglitibas-standartu. [Accessed: Feb. 15, 2025].

[31] "Informatīvais ziņojums 'Digitālās desmitgades stratēģiskais ceļvedis Latvijai līdz 2030. gadam.'" Available: https://tapportals.mk.gov.lv/legal_acts/82b52f77-febe-4480-ac95-c11eff9c283a. [Accessed: Feb. 15, 2025].

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 149-153

Modern Innovative Approaches of Domestic and Foreign Experts to Modernize the Physical Training of Female Servicewomen

Andrii Kalabskyi
Graduate student Department of Theory and Methods of Physical Education
Ivan Boberskyi Lviv State University of Physical Culture
Lviv, Ukraine
andrejkalabskij@gmail.com

Serhii Romanchuk
Department of Physical Education, Special Physical Training and Sports
Hetman Petro Sahaidachnyi National Army Academy
Lviv, Ukraine
romanchukserg13@gmail.com

Nataliia Sorokolit
Department of Theory and Methods of Physical Education
Ivan Boberskyi Lviv State University of Physical Culture
Lviv, Ukraine
sorokolit21@gmail.com

Artur Oderov
Department of Physical Education, Special Physical Training and Sports
Hetman Petro Sahaidachnyi National Army Academy
Lviv, Ukraine
stroyova@ukr.net

Orest Loiko
Department of Physical Education, Special Physical Training and Sports
Hetman Petro Sahaidachnyi National Army Academy
Lviv, Ukraine
oloyko1964@ukr.net

***Abstract* – The use of innovative approaches in military affairs allows achieving significant success both on the battlefield and in training. The world's leading armies are considering modernizing the physical training of female military personnel and have focused on finding ways to improve the physical fitness of female servicewomen. Unfortunately, the overemphasis in military history and legacy on aerobic fitness and "field expediency" as the primary criteria for training implementation has limited the extent to which the military has fully implemented state-of-the-art PT policies. This inherited approach can be problematic in fully enhancing women's ability to perform physically demanding combat tasks and can put the successful integration of women into ground combat MOSs at significant risk. *Purpose:* to get acquainted with the introduction of new ideas and technologies in the physical education of female servicemen in both Ukrainian and foreign armies and, based on the results obtained, to propose directions for improving the level of physical fitness of female servicemen of the Armed Forces of Ukraine. *Material and Methods:* Analysis of scientific literature and documentary sources on the problems of physical training of female servicewomen; generalization and systematization of theoretical knowledge related to the trends in the development of physical training of female servicewomen in the scientific and methodological literature. *Results:* Some Ukrainian scholars have considered the use of innovative approaches to improve the physical fitness of military personnel. The study found that the armed forces of the United States of America and the United Kingdom have created special research units that have been conducting in-depth research on the problems of physical training of female servicewomen in the modern army over the past ten years. The use of the following technologies has been established: information and communication, differentiated physical education, and health preservation technology. In addition, the above countries are developing a physical training strategy to optimize the performance of women servicewomen in combat professions. *Conclusions*. Having analyzed the scientific works of Ukrainian and foreign authors, it should be noted that in order to improve the level of physical fitness of female servicewomen, it is necessary to use technologies that allow taking into account the physiological characteristics of women and using the strengths of the female body when creating physical training programs for female servicewomen in combat specialties.**

Keywords – army, innovative approaches, female, physical fitness, servicewoman.

I. Introduction

In today's world, it is impossible to make progress in any field of human activity without applying innovative approaches.

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8474
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

The latest technologies created on a scientific basis allow achieving significant results, saving time and resources and producing a better and more reliable product. The use of innovative approaches in military affairs in modern armies of the world also takes place.

One of the peculiarities of modern armies is that women are allowed to master combat professions and serve in combat units, so leading armies have begun to apply innovative approaches to the physical training of female soldiers. Given that female servicewomen have to perform combat missions in accordance with the requirements of modern combat, there is a need to improve their physical fitness. In our opinion, one of the directions can be the modernization of physical training through modern innovative approaches used in physical education and sports [1].

Modern military affairs requires a high level of physical fitness from women servicewomen, especially for women who hold combat positions. Physical fitness is one of the key factors that determines the combat readiness and combat capability of a unit's personnel. Recent scientific studies show the need to adapt training programs to the physiological characteristics of women servicewomen serving in combat units [2]. In the process of identifying innovative approaches to improving the physical fitness of female servicewomen, a number of domestic and foreign scientists [3, 4] focused on finding ways to improve the content and forms of physical training of female servicewomen [5].

II. MATERIALS AND METHODS

The following research methods were used to analyze innovative approaches to the physical training of female servicewomen: analysis of scientific literature (review of works by domestic and foreign researchers on modern approaches to the physical training of female servicewomen) [6, 7, 8, 9], comparative analysis (study of physical training programs for female servicewomen in different countries and their effectiveness) [10, 11].

III. RESULTS AND DISCUSSION

In Ukraine, the following scholars have studied the implementation of modern innovative approaches of domestic and foreign specialists to modernize the physical fitness of female servicewomen: Oderov A. in his work “Innovative approaches to assessing the physical fitness of servicewomen in the system of professional training” [12].

The article proves that the system of assessment and testing of physical qualities of servicemen plays a significant role in the formation of professional abilities of military specialists. In order to assess the military applied skills of servicemen, a number of physical exercises have been substantiated and implemented, for which standards have been developed.

The development of physical exercises took into account the results of a survey of combatants who identified the main types of combat missions, namely: marching (30%), defense (19.2%), duty at checkpoints and protection of facilities (17.0%). The results of the exercise test made it possible to find out that the use of personal protective equipment and weapons contributes to the improvement of professional qualities. The authors [13] in their article “Fundamentals of Formation of Military Applied Skills of Officers through Orienteering” consider the improvement of military applied skills of the Armed Forces of Ukraine through the use of orienteering [13]. It is emphasized that regular practical training in terrain orienteering allows servicemen to move confidently in unfamiliar terrain and overcome various natural obstacles, receive and analyze relevant information, and make quick decisions in extreme situations. Romanchuk S., studied the specifics of women's physical training in the military forces of NATO countries and offers recommendations for improving the national system of physical training of ground forces [14].

Study the peculiarities of women's physical fitness and the volume of most physical activities, emphasizing the importance of a differentiated approach [15].

In our opinion, the main directions for improving the physical fitness of women in the Armed Forces of Ukraine are a differential approach (development of training programs that take into account the characteristics of the female body, with an emphasis on the development of functional strength, endurance and stress resistance), functional training (use of crossfit, bodyweight training and martial arts elements to improve overall physical fitness), rehabilitation methods (implementation of a program of recovery after physical exertion, including massage, yoga and technical [16, 17, 18].

In NATO countries and other developed countries, physical training for women in military units is based on scientifically sound approaches. Modern innovative methods include: gender-specific training programs (adapted sets of exercises that help to increase strength endurance without overloading the musculoskeletal system), digital technologies (use of mobile applications and specialized sensors to increase the level of physical fitness and load), multidisciplinary approach: involvement of physiologists, nutritionists, psychologists and sports doctors in the development of individual training programs, tactical fitness (focus on exercises that simulate real combat conditions, including moving with heavy equipment, overcoming obstacles and evacuating the wounded) [19].

The research [20] in “Physical training of cadets of military educational institutions of the Ground Forces of the Armed Forces of Ukraine” emphasizes the importance of taking into account the physiological differences of women when developing training programs.

In their study “Effects of Two Different Eight-Week Training Programs on Military Physical Performance” compare the effectiveness of different training programs for female military personnel [21].

A systematic review of the works of domestic and foreign researchers on modern approaches to physical training of military personnel In particular, the results of research in the field of military physical training, gender adaptation of training programs and the impact of innovative methods on the combat effectiveness of military personnel are considered.

After conducting a comparative analysis of physical training programs for female servicewomen from different countries and studying their effectiveness, we found that the US and UK armies have implemented comprehensive training programs focused on the development of endurance, strength and psychological training. The programs include high-intensity functional training (HIFT), the use of body monitoring technologies, and an adaptive approach to exercise [22].

The armies of Germany, France, and Canada use a multi-level training system that includes general physical, specialized, and combat training. Particular attention is paid to exercises to develop endurance and strength characteristics [23].

Physical training programs in Australia and New Zealand are actively implementing specialized programs for women, including strength training, flexibility development, and adaptation to physical activity in combat conditions. An important component is psychological training and recovery strategies [24].

The Israeli army has one of the most developed physical training programs for female soldiers in combat positions. Considerable attention is paid to the development of general endurance, functional strength and psychological stability. CrossFit and high-load training techniques are used [25].

Sweden, Norway, and Finland pay special attention to equal physical training of both male and female servicemen and women, integrating training that develops strength, endurance, and psychological stability. Particular attention is paid to maintaining the health of military personnel, their safety and injury prevention [26].

Ukraine is gradually adapting physical training programs for female servicewomen, based on the experience of foreign countries. In particular, training centers and higher military educational institutions are introducing functional training, gender-specific physical fitness testing, and gradual modernization of training programs [27].

Current research proves the effectiveness of high-intensity functional training (HIFT) for military personnel. Such training includes aerobic and strength exercises that increase endurance and overall physical fitness

Assessment of physical endurance, strength characteristics and injury rates. The studies have shown that: Physical endurance. Female servicewomen trained in functional training programs (HIFT) demonstrate increased aerobic endurance and adapt more quickly to combat loads compared to traditional programs. Strength characteristics. Analysis of data shows that specialized strength training programs contribute to the improvement of women's overall physical fitness, in particular, the development of muscular endurance of the lower body, which is critical for performing tactical tasks. Injury rate. Statistics show that the level of injuries among women servicewomen is higher when training programs do not take into account their physiological characteristics. Optimization of programs can reduce overload and injury by 20-30%. Physiological differences between men and women require adjustment of loads, focusing on the development of lower body strength, coordination and muscle endurance [28]. Studies show that specialized programs can significantly reduce the risk of injury among female military personnel.

The use of biometric sensors, body condition monitoring systems, and virtual training platforms helps to individualize the approach to military training and increases the effectiveness of training.

Some Ukrainian scholars have considered the use of innovative approaches to improving the physical fitness of military personnel. The study found that the Armed Forces of the United States and the United Kingdom have created special research units that have been completing in-depth research on the problem of physical training of women in the modern army over the past ten years [14], [25]. The use of the following technologies has been established: information and communication, differentiated physical education, and health preservation technology. In addition, these countries are developing a physical training strategy to optimize the employment of women servicewomen in combat specialties.

The analysis of the research sources showed that the Armed Forces of Ukraine do not have a thorough (comprehensive) approach to improving the physical fitness of female servicewomen through the introduction of innovative modern technologies. No state programs have been developed on the scale of the Armed Forces of Ukraine; there are only individual author's programs of scientists who propose to use them in training, both in specific specialties and branches of the armed forces, as well as in different categories (men and women) [7], [12], [28]. At the moment, the Armed Forces of Ukraine do not consider, create or produce special women's sportswear and footwear for training military exercises, actions and skills. In our opinion, the production and use of the following attributes could improve the level of physical fitness of female servicewomen.

To improve the effectiveness of physical training of women in the Armed Forces of Ukraine, it is advisable to [9], [11]: introduce modern technologies for monitoring physical activity: the use of biometric sensors and artificial intelligence for a personalized approach to training.

Thus, both domestic and foreign researchers are actively working to improve the physical training of women servicewomen by introducing innovative methods and approaches that take into account gender characteristics and modern requirements for military service.

IV. CONCLUSIONS

Physiological differences, in particular in the strength and power of the upper body between women and men, as well as the severity of combat-oriented professional requirements, in our opinion, put female servicewomen at a significant disadvantage, as the Armed Forces of NATO countries are introducing previously closed combat professional specialties (MOS) for women.

This inherent disadvantage can be greatly mitigated by implementing effective and comprehensive physical training (PT) regimens for women that target those components of physical fitness that are most critical to those tasks considered most important to a soldier's combat duties (i.e., strength and power).

After analyzing the scientific works of Ukrainian and foreign authors, it should be noted that in order to improve the level of physical fitness of female servicewomen, it is necessary to use technologies that take into account the physiological characteristics of women and replace the strength of the female body when creating a physical training program for female servicewomen in combat specialties.

REFERENCES

[1] D. Avzalova and V. Refel, "Physical training and sport of military personnel in higher military educational institutions of Ukraine and foreign countries," Graal of Science, no. 29, pp. 365-372, 2023. https://doi.org/10.36074/grail-of-science.07.07.2023.063.

[2] Y. Epstein, R. Yanovich, D. Moran, and Y. Heled, "Physiological employment standards IV: integration of

women in combat units physiological and medical considerations," Eur. J. Appl. Physiol., vol. 113, no. 11, pp. 2673-2680, 2013. https://doi.org/10.1007/s00421-012-2558-7.

[3] J. Greeves, "Physiological implications, performance assessment and risk mitigation strategies of women in combat-centric occupations," J. Strength Cond. Res., vol. 29, Suppl. 11, pp. 94-100, 2015. https://doi.org/10.1519/JSC.0000000000001116.

[4] C. Haddock, W. Poston, K. Heinrich, S. Jahnke, and N. Jitnarin, "The benefits of high-intensity functional training fitness programs for military personnel," Mil. Med., vol. 181, no. 11, pp. e1508-e1514, 2016. [Online]. Available: https://doi.org/10.7205/MILMED-D-15-00503.

[5] J. Hefley, L. Talbot, E. Metter, M. Lorenz, H. Shattuck, K. Romito, R. Heyne, and D. F. Bradley Jr., "Advancing readiness through military programs: An evidence-based practice perspective," Mil. Med., vol. 189, Suppl. 1, pp. 31-38, 2023. https://doi.org/10.1093/milmed/usad230.

[6] D. Karmon Dyches, K. E. Friedl, J. P. Greeves, M. F. Keller, H. L. McClung, M. S. McGurk, K. L. Popp, D. S. Teyhen, "Physiology of health and performance: Enabling success of women in combat arms roles," Military Medicine, vol. 188, no. 4, pp. 19-31, 2023. https://doi.org/10.1093/milmed/usac256.

[7] O. M. Loiko, "Using the experience of the North Atlantic Alliance Armed Forces in improving the system of physical training in the Armed Forces of Ukraine," in Young sports science of Ukraine. Collection of scientific articles in the field of physical culture and sports, Lviv: LDUFK, vol. 10, no. 1, pp. 360-365, 2006.

[8] T. R. Myers, M. G. Schneider, M. S. Schmale, and T. J. Hazell, "Whole-body aerobic resistance training circuit improves aerobic fitness and muscle strength in sedentary young females," J. Strength Cond. Res., vol. 29, no. 6, pp. 1592-1600, 2015. [Online]. Available: https://doi.org/10.1519/JSC.0000000000000790.

[9] O. Nebozhuk, A. Oderov et al., "Formation of military-applied skills of students of higher education institutions in the process of physical education," Volyn National University named after Lesya Ukrainka, vol. 1, no. 61, pp. 54-63, 2023. https://doi.org/10.29038/2220-7481-2023-01-54-63.

[10] B. Nindl, S. Eagle, P. Frykman, C. Palmer, E. Lammi, K. Reynolds, K. Allison, and E. Harman, "Functional physical training improves women's military occupational performance," J. Sci. Med. Sport, vol. 20, no. 4, pp. 91-97, Nov. 2017. https://doi.org/10.1016/j.jsams.2017.07.012.

[11] B. Nindl, B. Jones, S. Van Arsdale, K. Kelly, and W. Kraemer, "Operational physical performance and fitness in military women: Physiological, musculoskeletal injury, and optimized physical training considerations for successfully integrating women into combat-centric military occupations," Mil. Med., vol. 181, Suppl. 1, pp. 50-62, Jan. 2016. https://doi.org/10.7205/MILMED-D-15-00382.

[12] A. Oderov, "Innovative approaches to assessing the physical fitness of servicemen in the system of professional training," Sports Science of Ukraine, no. 3(73), pp. 26-31, 2016. [Online]. Available: http://sportscience.ldufk.edu.ua/index.php/snu/article/view/424.

[13] A. Oderov, M. Babych, O. Nebozhuk, V. Pylypchak, Pankevych, A. Guba, I. Shlyamar, O. Tymochko, A. Dunets-Lesko, A. Mandiuk, "Fundamentals of formation of military applied skills of servicemen by means of orienteering," Scientific Journal of the National Pedagogical Dragomanov University, vol. 8, no. 168, pp. 109-112, 2023. https://doi.org/10.31392/NPU-nc.series15.2023.8(168).21.

[14] A. Oderov, S. Romanchuk, T. Lyudovyk, I. Fishchuk, Ya. Svyshch, I. Pylypchak, T. Dukh, V. Lashta, "Improvement of special qualities of military personnel by means of physical education," Bulletin of Kamianets-Podilskyi Ivan Ohienko National University, vol. 26, pp. 135-140, 2022. https://doi.org/10.32626/2309-8082.2022-26.135-140.

[15] V. Klymovych, M. Korchagin,O. Olkhovyi, S. Romanchuk, A. Oderov, "The influence of the system of physical education of a higher educational school on the level of psychophysiological qualities of young people," SportMont Journal, vol. 17, no. 2, pp. 93-97, 2019. https://doi.org/10.26773/smj.190616.

[16] A. Oderov, O. Nebozhuk, O. Lesko, I. Pylypchak, O. Olkhovyi, A. Poltavets, V. Romanchuk, "Analysis of the dynamics of physical development of cadets as a result of the application of CrossFit equipment," Slobozhanskyi Scientific and Sports Bulletin, vol. 26, no. 4, pp. 133-140, 2022. https://doi.org/10.15391/snsv.2022-4.006.

[17] A. Oderov, M. Kuznetsov, S. Romanchuk, D. Pohrebniak, S. Indyka, N. Bielikova, "Analysis of the level of physical fitness of cadets of the Military College of Sergeants at the stage of primary," Sport i Turystyka. Środkowoeuropejskie Czasopismo Naukowe, vol. 5, no. 1, pp. 93-102, 2022. http://dx.doi.org/10.16926/sit.2022.01.05.

[18] O. Pervachuk, A. Oderov, V. Gunchenko, V. Ponomaryov, O. Nebozhuk, A. Melnikov, V. Lashta, V. Andreychuk, I. Romaniv, "Interrelation of military professional training and physical fitness of servicemen," Physical education, sports and health culture in modern society, vol. 65, pp. 10-17, 2024. https://doi.org/10.29038/2220-7481-2024-01-10-17.

[19] K. Phillips, A. Banaag, L. Lynch, H. Wu, M. Janvrin, T. Koehlmoos, "Comparison of musculoskeletal injury and behavioral health diagnoses among U.S. Army active duty servicewomen in ground combat and non-ground combat military occupational specialties," Mil. Med., vol. 187, no. 9-10, pp. 1024-1029, 2022. https://doi.org/10.1093/milmed/usac022.

[20] S. Romanchuk, "Physical training of cadets of military educational institutions of the Ground Forces of the Armed Forces of Ukraine," Monograph, 2012, p. 367.

[21] S. Romanchuk, S. Fedak, V. Afonin, O. Loiko, I. Fishchuk, "Physical training of cadets of higher military educational institutions based on the selective direction of professional education," Monograph, 2022, p. 386.

[22] S. Romanchuk, O. Nebozhuk, A. Oderov, M. Kuznetsov, V. Romanchuk, O. Boyarchuk, I. Tychyna, "Innovative research on the content of physical training in the armed forces of foreign countries as an element of training a military professional," Bulletin of Kamianets-Podilskyi Ivan Ohienko National University, Physical Education, Sport and Human Health, vol. 23, pp. 46-51, 2022. [Online]. Available: http://visnyk-sport.kpnu.edu.ua/article/view/253900.

[23] S. Romanchuk, Y. Svyshch, T. Shchur, A. Arabskyi, O. Borzilo, V. Bilyk, A. Oderov, "Physical training as the main criterion for assessing cadets' combat capability in the process of military professional activity," Scientific Journal of the Drahomanov Ukrainian State University. Series 15, Scientific and pedagogical problems of physical culture (physical culture and sports), vol. 12, no. 185, pp. 166-169, 2024. [Online]. Available: https://doi.org/10.31392/UDU-nc.series15.2024.12(185).35.

[24] L. Rybalko, "Directions of modernization of professional training of future specialists in physical culture and sports under martial law," Scientific Journal of the Mykhailo Drahomanov Ukrainian State University, Series 15, vol. 3K(176), pp. 404-409, 2024. [Online]. Available: https://doi.org/10.31392/UDU-nc.series15.2024.3K(176).89.

[25] [25] M. Santtila, K. Pihlainen, J. Viskari, and H. Kyröläinen, "Optimal physical training during military basic training period," J. Strength Cond. Res., vol. 29, no. 11, pp. 154-157, 2015. [Online]. Available: https://doi.org/10.1519/JSC.0000000000001035.

[26] [26] J. Vaara, J. Kokko, M. Isoranta, and H. Kyröläinen, "Effects of added resistance training on physical fitness, body composition, and serum hormone concentrations during eight weeks of special military training period," J. Strength Cond. Res., vol. 29, no. 11, pp. 168-172, 2015. [Online]. Available: https://doi.org/10.1519/JSC.00000000000010

[27] A. Andres, V. Kryzhanovskyj, I. Krasovska, O. Bodnarchuk, O. Khanikiants, A. Mandiuk, O. Rymar, A. Solovey, N. Sorokolit, M. Stefanyshyn, M. Yaroshyk, "The influence of agility indicators on the formation of vocational readiness in law enforcement officers," Society. Integration. Education: proceedings of the International Scientific Conference, vol. 1, pp. 165–179, Rēzekne, 2023. doi: https://doi.org/10.17770/sie2023vol1.7105

[28] A. Andres, A. Sorokolit, A. Mandiuk, O. Rymar, O. Khanikiants, "The impact of sports activities on the psycho-emotional state of cadets in higher education institutions during wartime," Environment. Technologies. Resources. Proceedings of the International Scientific and Practical Conference, vol. 4, pp. 23–26, Velikoternovo, 2024. doi:https://doi.org/10.17770/etr2024vol4.8206

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 155-161

Criminal Law Education as a Component of the National Security System of the Republic of Bulgaria

Lyuboslav Lyubenov
Universty of Ruse -
„Angel Kanchev"
Ruse, Bulgaria
lvlyubenov@uni-ruse.bg

Abstract- **Criminal law is deeply connected with human nature, because it indicates the natural striving of the individual after safety and prosperity. Criminal law is a civilized form of measuring and limiting the fear of violence and arbitrariness in the human community. Insofar as criminal law practice is a mechanism for creating an assessment and a fair resolution of a dangerous life conflict, it is also a mechanism for creating safety, reassurance and satisfaction of the socially organized person. Criminal law education is an important component of the national security system of the Republic of Bulgaria. With its help it is possible to successfully train and educate human resources supposed to recognize, realize and manage the emerging risks, especially (but not only) in the justice, judicial and educational systems of the state. The products (legal acts/deeds) of a knowledgeable person in the field of criminal justice are of universal value and usefulness. It could and should be successfully invested in the sphere of national security as public welfare through criminal law education. Quality criminal law education accelerates, enriches and expands the field of application of the fight against crimes as one of the important modern tests in the rule of law. In this sense, it contributes in its own way to the understanding of the dilemma, levels, classification and management of national security in the rule of law. By the way, the rule of law is both a goal and a means of national security. Improving the quality of criminal law education in the conditions of a changing social environment leads to a budget and safe increase in the quality and quantity of the national security in the Republic of Bulgaria. Educating knowldeable and decent citizens increases national security by reducing mistrust between individual members of society. With some reservations - an educated person is more reasonable, more responsible, more creative and more predictable than an uneducated one.**

Keywords - education, security, criminal law, criminal process, science.

I. INTRODUCTION

The modern world is complex and dynamic, and therefore problematic. The preservation and development of the world, therefore, is based on the possibility of a successful solution of the problems arising and modifying within it. Problem solving, however, is not possible without knowing both the world and the problems themselves, i.e. without the formation of knowledge. This is valid even when there is a possible conclusion that a problem does not actually exist (i.e. an imaginary problem). Hence, the process of creating, preserving, enriching and teaching knowledge is a key issue to the evolution of the world. This is how the creation of quality education (as a strategic task) in itself ensures the achievement of security in the world (as a strategic goal). According to this strategic goal, appropriate resources (including human resources) have to be created, organized and used. There is no other way. It is no coincidence that Stoyko Stoykov concludes "... We can no longer arm ourselves with our own abilities and imagine that they will be enough for us. Security requires the continuous creation and development of capabilities ... because now the goal determines the resources, not the resources – the goal. Facing certain problems, we ought to find solutions, and not seek for problems that meet our requirements, because the search for scientifically based solutions is possible only if we develop not what we know about, but we know and are prepared for what we work for"[1]. Relatively speaking, the more scientific knowledge is, the more

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8471
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

reasonable is the state of affairs recommended by it. The better knowledge is taught, the better the practice is facilitated. Hence, the more knowledgeable a person is, the better he does in solving problems and creating welfare for others. Transferred to the sphere of national security, these judgments mean that education is a strategic category. This is because as priority, through education, respectively through criminal law education, knowledgeable people are trained who, through their activities, are able to personally and realistically create national security in the rule of law. The products (legal acts/deeds) of the competent person in the field of criminal justice are of universal value and usefulness. It is possible and should be successfully invested in security as a kind of welfare, not exactly as a service to citizens through criminal law education. And this is the most desirable and most valuable aspect in the protection of the individual, the society and state nowadays [19]. In support of this statement it is enough to point out what Nikolay Slatinski stated: "the distribution of welfare is based on the principle of unconditionality, of pure justice, i.e. everyone receives his share from it. And the distribution of this service is related to the operation of the principle of conditionality, of criterion injustice" [2].

II. Materials and methods

What has been said so far makes it possible to understand the purpose, subject matter and tasks of this report. Namely The aim is to briefly approbate criminal law education as an important component of the national security system of the Republic of Bulgaria. To achieve the goal, it is necessary to perform the following tasks:

- To reveal the role of the positive criminal law in the national security system of the Republic of Bulgaria.
- To develop and illustrate the relationship between the quality of the criminal law education and the quality of the national security in the Republic of Bulgaria.
- To look for and explain the current problem of the criminal law education in the Republic of Bulgaria.
- To propose possible solutions for improving the teaching of criminal law in the higher schools of the Republic of Bulgaria.

The subject of the research in this report is criminal law education in the higher schools of the Republic of Bulgaria and its reflection on the national security system of the Republic of Bulgaria. The following scientific methods have been used to perform the tasks referred to: normative, logical, systemic and interdisciplinary. Only after examining the subject of research, mentioned in the title, through these methods can the desired benefit from the report be obtained, namely to prove and recommend that the improvement of criminal law education will lead to the enhancement of the national security system of the Republic of Bulgaria.

III. Results and discussion

Before proceeding to the solution of the tasks set and in compliance with the maxim omnis definitio periculosa est (meaning from latin- any definition is dangerous) it is appropriate to draw up a 'small chart' of the basic concepts frequently used in the report. The notion is about the concepts: security, risk, criminal law education, the place of criminal law education in the security system of the Republic of Bulgaria and criminal law.

First, the content of the concept of security should be specified. In this report, it is used in its possible and conceivable meaning in the broadest sense of the word, not in its deeper and more precise meanings in relation to the object of security science. This is imposed by the subject limitation of the publication set out in the very title. Certainty does not mean a state of absolute safety, protected safety, relative security, or transformational security [2]. Security is conceived more generally as a state of protection against influences that are detrimental to the equilibrium or to the very existence of the system (human being, society, state). I accept that conservation is the prevention or successful management of already allowed internal and/or external influences on the balance of the system [2]. It is useful to add that the modern comprehension of strategic security management requires not only continuous efforts to improve the formation and implementation of security policies, but also new approaches and specific solutions for modernizing the security system, making it adequate to the requirements of the dynamic security environment [3]. The development of such policies ought also to be consistent with the pace of change in security on the territory of the EU [4].

A certain factor (group of factors) could be identified with the concept of risk, which could manifest itself and threaten the equilibrium or existence of the system with measurable probability. Possible factors could be: processes, phenomena, conscious/unconscious human activity, respectively lack of the latter and so on.

Criminal law education here means a purposeful process of selection, systematization, lecturing, learning and acquisition of knowledge and skills about the essence, effect and consequences of the norms of the criminal and criminal procedure law of the Republic of Bulgaria.

The place of criminal law education as a specific concept in the national security system of the Republic of Bulgaria is conceivable and quickly discoverable through the scheme of the five levels of security developed by N. Slatinski [2]. Through criminal law education, security is produced predominantly for the subjects of the first three levels and ancillary (indirectly) for the subjects of the last two levels of security. Criminal law education, therefore, serves more to fathom and increase the protection of the individual, society and the state, and less to protect the community of states and the world as a whole. Metaphorically speaking, within some space boundaries, criminal law education "sits" with the individual, society and the state, both separately and simultaneously. And

quite naturally – criminal law and criminal procedure law are domestic legal branches with minimal direct global (non-state) manifestation.

In order to evolve in modern conditions, the system of education, training and research in the field of security should first of all be adaptable, i.e. able to change in order to respond to the changes in the security environment. Change is not just one of the most important processes in an organization, but an opportunity for its active and effective participation in this change [5].

In the following lines, for brevity and greater clarity, the term criminal law as general and expressing the totality of the substantive and procedural criminal law of the Republic of Bulgaria will be used. Although they exist independently as two separate legal branches, they are inextricably linked, because substantive criminal law without criminal procedure (in legal theory, the phrase criminal procedure is used as a synonym for the phrase - criminal procedural law) is meaningless, and the criminal process without substantive criminal law is pointless.

A. Criminal Law as a Positive Law.

Criminal Law as a Positive Law, [15] i.e. as a written law (a set of legal norms in force united in a system) that regulates certain social relations is important for the national security of the country by its very existence. This is so for three reasons.

First, criminal law is deeply connected with human nature, because through it the natural striving of the individual for safety and prosperity has always been reproduced. Criminal law is a civilized form of measuring and limiting the fear of violence and arbitrariness in the human community. Insofar as criminal law practice is a mechanism for creating an assessment and a fair resolution of a dangerous life conflict, it is also a mechanism for creating safety, reassurance and satisfaction of the socially organized person.

Secondly, it is evident from Art. 1 of the Criminal Code that criminal law has a protective function. It protects the individual, society and the state from criminal encroachments. The structure and content of criminal law provisions are directly determined by its protective (defensive) function [6], [12]. The outline of the essence, limits and direction of the protective function of the criminal law is achieved through the Criminal Code. The Code defines which socially dangerous acts are considered crimes and what penalties are imposed for them. Moreover, criminal law educates the protection of national security. To understand this, it is enough to point out the following thought of Rumen Markov: "By prohibiting the commission of crimes under fear of punishment, the criminal law exerts on the psyche of citizens a general educational (informational) and warning-deterrent effect in order to motivate them to refrain from crime. The general educational impact of the Criminal Code is based on information about the actual social nature of the acts declared to be crimes. Each crime is a socially dangerous act. By emphasizing their public danger, the Criminal Code educates the understanding of the categorical inadmissibility and reprehensibility of committing criminal acts. The warning-deterrent effect, in turn, is based on the anticipation of the punishment laid down by law and the warning that it will be imposed when the crime is committed" [6], [13], [14]. In summary - Criminal law regulates a type of conduct that is too dangerous for the national security, declaring it to be criminal and punishable, also instructs for the individual to refrain from undertaking it in terms of objective reality. Tis is considered to be useful for the national security.

Third, the actual (regulating in the narrow sense of the word) manifestation of the protective function of criminal law is achieved through the fulfillment of the tasks of the criminal process. The fulfillment of the tasks of the criminal process is an expression of the understanding that when the preventive effect of the protective function is actually neutralized by the commission of one or more crimes by one (at least) criminally responsible person, it is necessary to proceed to subsequent regulation of the offender's behavior, namely - exposing the guilty person and imposing a fair punishment. The criminal process is a way to realize the content of the substantive criminal legal relationship. When talking about criminal process, it must be borne in mind that, as part of the state activity, that it is always related to the nature, tasks and organization of the state itself. That is why the content and arrangement of criminal procedure institutes always follow and further develop the logic of those principles, methods and forms of work that characterize the state organization at a given historical moment. Therefore, the criminal process is always bound by significant state policies. Moreover, it is an instrument for the implementation of the state penal policy. In this line of thought, the norms of criminal procedure (consciously or not) express part of the state policy in the field of national security.

The tasks of the Bulgarian criminal process are two in number – main and immediate. They are regulated by law in Art. 1 of the CPC (Criminal Procedure Code of the Republic of Bulgaria).

In Art. 1 para 1 of the CPC, the legislator determines the immediate task of the process. It is expressed in the detection of crimes, exposure of the guilty and the correct application of the law. The main task of the process, on the other hand, is incorporated in Art. 1, par. 2 of the CPC. The legislator has ordered that the main task of the process is to ensure protection against criminal attacks concerning the Republic of Bulgaria, against the life, freedom, honor, rights and legitimate interests of citizens, as well as the rights and legitimate interests of legal entities, and assistance in preventing crimes and strengthening the rule of law. The main task is achieved by completing the immediate task [7], [17], [18]. This means protection of the Republic of Bulgaria, individual citizens and legal entities from criminal encroachments, as well as strengthening the trust in the law and law enforcement

only by detecting crimes, by exposing the guilty and by correctly and fairly applying the law in each possible criminal case. Criminal procedure provides protection of the national security through effective and fair sanctioning of its violators! In a state governed by the rule of law, this ought always to be conducted through the precise, fair and justified application of clear and expertly (scientifically) confirmed legal regulations.

In summary, with the help of positive criminal law, in a legal way and with legitimate coercion, intervention with criminal attacks on the national security of the Republic of Bulgaria is prohibited and sanctioned. Criminal encroachments are only one of the possible threats to national security, but very serious and with a steady probability of manifestation. Hence, criminal law is important and should be amended and further developed de lege ferenda so as to effectively contribute to limiting and managing the risk of committing crimes in the Republic of Bulgaria. For cognitive purposes, it should be noted that the norms of international criminal law could provide protection to the international security.

B. Criminal Law Education and Its Role in the Protection of the National Security of the Republic of Bulgaria.

Education is one of the fundamental values of the modern world and without it there will be no foundation on which society might step in order to move forward. Modern organizations of science, education and qualifications in the security system are becoming more and more dependent on knowledge, because they have to become "knowledge factories" and their main product is mainly ideas, not material products. The key to success is the fundamental transformation of the role of science in our academic life by creating a sustainable institutional model for national security system research [8].

Criminal law education is an important component of the national security system of the Republic of Bulgaria, because with its help human resources could be successfully trained and educated. These resources ought to recognize, realize and manage the emerging risks, especially (but not only) in the justice, judicial and educational systems of the state. In other words, only with the help of criminal law education it is possible for human resources to be developed in the area of understanding and strictly applying the norms of positive criminal law in the environment of changing national security. Criminal law education as a purposeful process of transferring knowledge from the trainer to the trainee and aims to form in the latter ideas and views about the actual content and manifestation of criminal law norms, as well as readiness for fair action in accordance with these ideas in the objective legal world. Only in this way, through the knowledge and understanding of the actual meaning of the norms of criminal law, an adequate and solid discerning in connection with protection of the national security from criminal encroachments can be established. Criminal law education, therefore, provides invaluable knowledge for a desired impact on national security through the norms of criminal law. Therefore, accelerating, enriching and expanding the fight against crimes in the rule of law is a function of high-quality criminal law education. Without it, this struggle could hardly be developed into a goal and could hardly evolve thoroughly. To summarize, without criminal law education, it is almost impossible to develop a skill to counteract crime. This skill is especially valuable because, even if left "in the hands" of a single citizen, it can produce security for the majority of citizens. Through it, security is created and protected as a benefit for the whole society! Hence, the lack of legal knowledge and skills to counteract crimes always worsens the protection of national security [16]. It would not be an exaggeration to conclude that **legal incompetence is a serious risk to the national security system**.

At present, higher education institutions are the main place where criminal law education is established and received. Lecturers at higher education institutions are entrusted with minimizing the weaknesses and maximizing the strengths of criminal law education. To date, the problems of criminal law education are actually a private manifestation of the problems of the educational system in the Republic of Bulgaria. If the main problem of the educational system is emphasized, it cannot but be noticed that it manifests itself as such (main) in the conduct of criminal law education in higher schools. In my opinion **This problem is expressed in the reproduction of training, which is focused more on providing ready-made useful information to learners, and less on providing information and skills for independent interpretation and finding useful information.** The emphasis is on knowledge instead of seeking for awareness and comprehension! Comprehension is a larger category. It contains a system of knowledge related both to each other and to real life and state policies implemented in it. S. Stoykov has reached a similar conclusion (albeit on a different occasion): "In Bulgaria, the reform in education is concerned with what to learn, instead of how to learn... The learning process should be centered around the student, not around the teacher... Students are asked to reproduce the material from the textbook, and not to debate ideas and alternatives for development. Lectures are supposed to provide answers to all questions..." [9]. Criminal law education should therefore be organized in such a way as to influence with knowledge not only on criminal law norms, but also on their interaction with the components of the national security system in the state.

The criminal law education itself is a component of the national security system, which is located and functions in view of its other components. For example, education itself is a component of the national security system, which is located next to and functions alongside social and health security, which are also components of the country's national security system. The idea that criminal law education is a component of the national security system, through which security is produced as a benefit for all citizens, leads to a fair conclusion in financial terms. The state is interested in allocating more money to good teachers and students! Thus, money "follows" the competent and capable, but also the interest of the entire

Bulgarian society! It is important that well-trained experts are well paid, because well-paid unprepared experts do nothing to protect national security! The arbitrary and random provision of money in the education system does not guarantee the increase of security in society. And here is the time to recall the security dilemma – it is not true that whenever a system (state) invests in its security, including by increasing monetary resources, it necessarily receives more security [9]. And one more thing, priority threats require ideas and careful reforms in investments, due to the limitations and the tendency to reduce national resources [10]. Increasing the quality of criminal law education through the comprehensive stimulation of those who know in the educational system (instead of everyone employed in it) is cheaper and more justified, because a person who is valued with dignity is more productive and more interested in the future. In this regard, some important recommendations for improving the current quality of criminal law education in the country's higher education institutions will be provided below.

First, the number of exercises for the interpretation of criminal law norms should be increased in the curriculum. Students should be encouraged to analyze and disclose the content of criminal legal relations independently. This will give them the opportunity to fully discover and comprehend the relationship between the norms of criminal law and the norms of other legal branches. In this way, the complex influence of the Bulgarian legislation on the national security system can be traced and directed.

Secondly, to encourage the resolution of criminal cases that illustrate well the relationship between criminal law and the protection of national security. This is not particularly difficult, given that there are entire sections in the Criminal Code with crimes against different levels of security. For example, crimes against the republic, crimes against the person, crimes against the rights and freedoms of citizens, generally dangerous crimes, etc.

Thirdly, to assign more independent work to students, which should include answers to questions of an interdisciplinary nature. For example, preparing and delivering reports, presentations and essays on the application of legal institutions that regulate public relations in the field of national security. A person learns well while teaching!

Fourthly, to expand the influence of legal clinics in universities, as students acquire the habits of legal work with citizens on legal problems from real life cases there. Responsiveness, responsibility and empathy for fellow citizens in need is cultivated in such places.

Fifth, to increase the internship time of students under the supervision of a habilitated person in the justice system. In this way, it is more understandable and faster to observe, study and include in the fight against crime.

Sixth, students should be more often enrolled in existing and future projects in the field of justice or national security with specific tasks according to their current preparation. For example, students can engage in the preparation of: surveys, draft documents, short analyses, translations, etc. All this adds not only knowledge and skills, but also self-confidence due to the general commitment to tasks with real experts from theory and practice.

Seventh, to stimulate students who excel in high results during their studies or in student programs for educational exchange, scientific student conferences, contests and competitions. Such students can be stimulated with: generous cash prizes, sponsored access to world databases with scientific and educational content, internships in significant state and private structures, facilitated conditions for applying for PhD students and junior experts in practice. The same attitude can be applied to high-achieving lecturers.

Eighth, more guidance to students in terms of education should be applied. For this purpose, they should be directed to considering reality as it is. Thus, students learn to separate the illusory from the real problems and undertake appropriate behavior. This increases the desire to get in touch with reality and builds confidence in the face of all its changes. In other words, an ambition for development is in the process of developing. A similar conclusion is made by S. Stoykov: "education is a single purposeful process of upbringing, training and acquisition of a set of knowledge, skills, values, social beliefs and habits, for the formation of the mind, character and physical abilities of a person, as well as the transmission of knowledge accumulated over generations" [11].

Ninth, to approach students more individually, depending on their strengths and talents. Thus, each of them will get to know each other more easily and it will be easier to form faith in themselves. They will get used to relying first on themselves and in case of need- on others. Such people are truly capable of connecting with other people and taking care of them.

Tenth, to pay more attention to building leadership qualities in students. In the modern world, difficulties are diverse, multidirectional and daily. Everyone should be able to manage their own difficulties. Difficulty should not be denied and deviated, but accepted and overcome (as far as and if possible), because in difficulty the personality grows!

Eleventh, when evaluating students after the exam, their activity and work during the academic semester should be considered. Thus, students are taught to organize their goal around work, not their work around the goal. Work prepares a person for life, not just for the moments chosen by him. Like an exam, for example!

IV. CONCLUSION

From all that has been said so far, the following important conclusions can be drawn which are a direct result from it and prove all formulated tasks:

- Criminal law education is a strategically important component of the national security system of the Republic of Bulgaria. The human resource who has received a good criminal law education develops and applies legal norms consistent with the protection of national security.

- Criminal law education contributes to the comprehension, affirmation and reproduction of security as a benefit for the Bulgarian nation.
- Without criminal law education, it is almost impossible to develop the skill of opposing crime, as the main threat to the modern rule of law and its society.
- Poor criminal law education leads to poor protection of individual, group and state security.
- Improving the quality of criminal law education in the conditions of a changing social environment leads to a cheap and safe increase in the quality and quantity of national security in and in the Republic of Bulgaria.
- Criminal law as a valid written law is important for the national security of the country, if only by the fact of its existence [20].
- Bulgarian criminal law education is not unproblematic. It encounters solvable problems. The solution of these problems should be made a priority because it will lead to the creation of individuals who are knowledgeable, responsible, confident and unyielding in the face of life's difficulties.
- The tutoring of educated and decent citizens always increases national security by reducing mistrust between individual members of society. With some reservations - the educated person is more reasonable, more collective, more creative and more predictable than the uneducated!

It should be explicitly stated that the report has achieved the goal stated in the title, namely, it has proven the statement that criminal law education is an important component of the national security system of the Republic of Bulgaria. The scientific benefit of proving this connection lies in the fact that this is how the improvement of criminal law education is understood and recommended as an effective tool for increasing national security, which has a generally valid utility for Bulgarian citizens. The study is also useful in that it outlines specific problems facing criminal law education together with their solutions. This also contributes to the correct understanding and overcoming of basic problems that affect the complex concept - national security, and not only the national security of the Republic of Bulgaria. The theoretical study is the first (new) of its kind on the territory of the Republic of Bulgaria.

ACKNOWLEDGMENTS

This research is supported by the Bulgarian Ministry of Education and Science under the National Program "Young Scientists and Postdoctoral Students-2"

REFERENCES

[1] S. Stoykov, Strategic Management of Knowledge in the Security and Defense System. Ed. "Knowledge Society Institute", Sofia, 2012, p. 128-129.

[2] N. Slatinski. The risk: the new name of security. Sofia: East-West, 2019, p. 378; p.380; p. 384-385.

[3] Stoykov, S., Risk management as a strategic management element in the security system, International Conference on Creative Business for Smart and Sustainable Growth, CreBUS 2019, March 2019, Article number 8840098, Category number CFP19U17-ART; Code 152084, ISBN: 978-172813467-3, DOI: 10.1109/CREBUS.2019.8840098

[4] G. Belova, Y. Kochev. "Challenges Facing Bulgaria's EU Presidency within the Context of Other New Member States' Experience". Balkanistic Forum Journal vol.1, 2018., p.270.

[5] Stoykov, S. (2024). The system of education, training and research in the field of security - managing change through experience and knowledge, ETR, vol. 4, pp. 269–274, Jun. 2024, doi: 10.17770/etr2024vol4.8213.

[6] R. Markov. Criminal Law of the Republic of Bulgaria – General Part. Sofia: Ciela, 2022, pp. 23-29.

[7] S. Pavlov. Criminal Procedure of the Republic of Bulgaria – General Part. Sofia: Sibi, 1996, p. 35.

[8] Stoykov, Stoyko ,,Scientific Knowledge - Source of a Competitive Advantage in Security, Published: 2018 in International Conference on High Technology for Sustainable Development (HiTech), ISBN: 978-153867039-2, DOI: 10.1109/HiTech.2018.8566548

[9] S. Stoykov. A dilemma of (not) security and the added value of security education. Scientific Journal "Security and Defense", 2022, p. 68; p.60. https://doi.org/10.70265/KRBW7556

[10] S. Stoykov. The System of Education, Training and Research in The Field of Security-Managing Change Through Experience And Knowledge. ENVIRONMENT. TECHNOLOGIES. RESOURCES. (2024). Proceedings of the International Scientific and Practical Conference, p. 273. https://doi.org/10.17770/etr2024vol4.8213

[11] Stoykov, Stoyko; Petrova, Elitsa, Situation Analysis of the Security Education and Training System in the Republic of Bulgaria, Vojenské rozhledy. 2023, 32 (2), Page Range: 67-82, ISSN 1210-3292 (print), 2336-2995 (online), DOI: 10.3849/2336-2995.32.2023.02.067-082,WOSUID: WOS:001016562500005

[12] N. Dolapchiev. Criminal Law. Common Part. Sofia: BAS Press, 1994, pp. 64-65.

[13] A. Stoynov. Criminal Law. Common Part. Sofia: Ciela, 2019, pp. 37-39.

[14] A. Gerginov. Criminal Law. Common Part. Sofia: Sofi-R, 2009, pp. 9-28.

[15] A. Gerginov. International Collaboration in Criminal Cases. Sofia: Sofi-R, 2012, pp. 9-14.

[16] I. Salov. Actual Problems of Criminal Procedure Law. Sofia: Nova Zvezda, 2014, pp. 108.

[17] N. Manev. Development of the Reform of the Criminal Process. Sofia: Ciela, 2018, pp. 10-18.

[18] M. Chinova, G.Mitov. Lections course in Criminal Procedure Law. Sofia: Ciela, 2021, pp. 30-32.

[19] Panteleeva, V. "The Tax Payers' Rights in Changing Society and Digital World" PROCEEDINGS OF UNIVERSITY OF RUSE - 2021, (2021):67-69, https://conf.uni-ruse.bg/bg/docs/cp21/7.1/7.1-9.pdf

[20] Lyuboslav Lyubenov "DOMESTIC LEGAL MEASURES FOR INCREASING SECURITY IN THE BLACK SEA REGION" Научно списание "Сигурност и отбрана", бр. 2 (2024): 9-18. DOI:10.70265/VIRM1297

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16-th International Scientific and Practical Conference. 2025. Volume V, 163-170

The Dynamics of Military Security – Challenges and Forecasts in the Conditions of Global (in)Security

Rumen Marinov
Security and Defense Faculty
Vasil Levski National Military University
Veliko Tarnovo, Republic of Bulgaria
ramarinoff@gmail.com

***Abstract*— This study focuses on transforming military security in the context of globalization, technological advances, and emerging threats. The concept of "military security" reflects the complex and dynamic nature of the contemporary global security environment, which has evolved from the traditional protection of territorial borders and populations to integrated strategies encompassing new threats, such as cyberattacks and hybrid conflicts. The study examines five key factors shaping new approaches to military security: technological advances, geopolitical dynamics, emerging threats, societal changes, and the need for adaptive and comprehensive solutions. It concludes by emphasizing that contemporary military security requires innovative and global approaches to address the challenges of a dynamically changing world.**

Keywords – military security, globalization, cyberattacks, hybrid conflicts, geopolitical transformations

I. Introduction

Although the importance of security in the modern world is widely recognized, there is a significant gap in the scientific literature on the interaction between traditional military threats and new, non-traditional challenges (such as cyberattacks, climate change, and hybrid warfare) in the context of global insecurity. Most existing studies consider military security separately from other dimensions, leading to fragmented analysis and limited predictive value in shaping comprehensive security policies.

The present study aims to fill this gap by analyzing the dynamics of military security in global (in)security through a unified approach that includes both classic military aspects and contemporary risks and vulnerabilities.

In the contemporary global context, security occupies a key place, especially against the backdrop of conflicts such as those in Ukraine and the Middle East. Despite the wide academic attention on traditional military security, there is a clear gap in terms of its overall interaction with emerging and non-traditional threats – cyberattacks, climate crises, hybrid warfare, and information impact. Much of the existing literature focuses on individual aspects of security, thus ignoring the complex and interconnected nature of contemporary threats.

The present study aims to overcome this gap by offering a systematic analysis of the dynamics of military security in the context of global (in)security, through an interdisciplinary approach. The study examines the classical military aspects and their interrelation with geopolitical, technological, and environmental factors, which are increasingly becoming catalysts of uncertainty.

II. Materials and Methods

The study uses combined methods to analyze military security in the contemporary global context. A literature review of theoretical and empirical sources is conducted, and documents and strategic reports of governmental and international organizations are examined. Case study analyses and comparative analyses of strategies of different countries and organizations provide examples of emerging threats. The Saati method (AHP) is also applied for hierarchical structuring and assessment of the importance of factors affecting the development of sound security strategies such as technological progress, geopolitical changes, and new threats.

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8467
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

III. RESULTS AND DISCUSSION

In the modern world, military security is subject to continuous changes, determined by four interrelated factors depicted in Figure 1.



Fig. 1 Challenges to military security

Technologies such as artificial intelligence and autonomous systems are significantly changing the way we wage war and provide defense, expanding both offensive and defensive capabilities. Geopolitical changes are leading to new strategic alliances and shifts in the global balance of power, requiring new approaches to national and international security. The dynamically evolving security environment and the expansion of combat domains increase the degree of uncertainty in military operations [1]. At the same time, emerging threats such as cyberattacks, terrorism, and climate change require integrated strategies that encompass not only military but also economic and social aspects of security. Societal changes, including demographic and political transformations, influence national strategies, emphasizing the need for social stability and effective interaction between the state and citizens. All these factors emphasize the need for complex, global, and adaptive solutions to ensure security in an increasingly unpredictable world.

The first factor – *technological progress* is represented by the rapid development of areas such as artificial intelligence (AI), cyber capabilities, space technologies, and autonomous weapons systems. The modern security environment and dynamic changes on a global scale require the use of alternative and modern methods of conducting and ensuring combat operations in different environments [2]. These innovations are transforming the nature of military security, introducing new forms of warfare and operational approaches. On the one hand, technologies expand the range of potential threats – for example, through cyberattacks or the use of unmanned aerial systems that are programmed to perform tasks that are potentially dangerous to humans but can also be remotely controlled [3]. On the other hand, they provide tools for more effective protection, such as improved early warning systems, cyber defense, and adaptive military strategies. Technological developments also highlight the need for international regulation and ethical standards to avoid escalating conflicts and unmanageable risks.

The second factor – geopolitical dynamics involves the emergence of new centers of power and the formation of alliances that can lead to unforeseen changes in global security. Changes in the balance of power are manifested through the transformation of traditional alliances and the rise of new powers. These processes require a rethinking of strategic approaches to military security, taking into account both cooperation and potential conflicts between states. Successful management of geopolitical changes depends on the ability to anticipate and adapt to new realities on the international stage.

The third factor – *emerging threats* such as cyberattacks, disinformation, terrorism, and climate change require more holistic strategies for military security. These threats not only go beyond traditional military approaches but also require integration between different spheres of security – economic, social, and environmental. Effectively dealing with them implies international cooperation, information exchange, and adaptability to new forms of risks. Protection against these threats includes both technologies and strategic policies that strengthen the resilience of states and societies.

The fourth factor – societal changes, demographic transitions, and political movements – also have a significant impact on priorities and approaches to national security. The increasing importance of social stability as a component of military security highlights the need for a balanced approach to economic and social policy. Demographic changes, such as an aging population or increasing numbers of migrants, can pose new challenges in resource allocation and maintaining public order. Political movements and changes in citizens' perceptions of security may require a readjustment of national strategies to respond to new realities and expectations. Efforts to strengthen social cohesion and build trust between the state and society are becoming increasingly crucial in ensuring the sustainability and effectiveness of military security.

The formula can be expressed as follows:

$$\boldsymbol{S} = \sum_{i=1}^{n} \boldsymbol{wi} \,.\, \boldsymbol{xi} \qquad (1)$$

Where:

– $\boldsymbol{S}$ is the overall assessment of the impact on military security.
– $\boldsymbol{n}$ is the number of key factors.

To analyze the impact of these key factors on military security, the formula according to the Saati method can be adapted, which uses the Analytic Hierarchy Process (AHP) for decision-making under multi-criteria situational factors.

$\boldsymbol{wi}$ is the weights, which must satisfy the condition to guarantee normalization, where:

$$\sum_{i=1}^{n} \boldsymbol{wi} = 1 \qquad (2)$$

xi is an estimate of the i-th factor (in the range of 1 to 9).

Example: If the factors and their weights are:
– technological progress ($w_1 = 0.3$, $F_1 = 8$),
– geopolitical dynamics ($w_2 = 0.25$, $F_2 = 7$),
– emerging threats ($w_3 = 0.3$, $F_3 = 9$),
– social changes ($w_4 = 0.15$, $F_4 = 6$),
then:

S=(0,3 x 8)+(0,25 x 7)+(0,3 x 9)+(0,15 x 6) = 7,55

This provides a generalized assessment of the impact of factors on military security.

Forecasting the evolving dynamics of military security

Forecasting the dynamics of military security is a complex process that requires the integration of multiple interrelated factors in the context of global and regional changes. In the modern world, marked by increasing uncertainty and constantly evolving threats, military security plays a key role in preserving the stability and sovereignty of states. The dynamics of this area are shaped by emerging factors such as technological advances, the expansion of hybrid conflicts, and the need for global coordination. This task is particularly challenging due to the high degree of uncertainty characteristic of the modern security environment and the possibility of unforeseen events that can significantly affect the global balance of power. The development of military strategies and capabilities is no longer limited to traditional dimensions of force but requires an integrated approach, encompassing innovation, sustainability, and multilateral cooperation.

Challenges defining the future dynamics of military security include: **adoption and deployment of new technologies, hybrid warfare, resilience and adaptability, multi-domain operations, and strategic alliances and partnerships.** These challenges require rethinking traditional approaches to military security and investing in innovation, coordination, and strategic cooperation. This analysis focuses on key aspects of these challenges and explores ways to address them through adaptability and strategic planning.

The Saati method is an effective tool for assessing the importance of different criteria and for determining the strategies that can lead to optimal results in conditions of global (in)security. By comparing each criterion against the others on a predefined scale (e.g. from 1 to 9), the weights of the criteria are calculated. This methodology provides a data-based and objective approach for the analysis and selection of strategies and policies, especially in the context of dynamic military security.

In this example, the method has been adapted to address multi-criteria challenges. The formula has been revised to provide a structured and integrated approach to evaluating different options based on multiple criteria. It can be represented as follows:

$$\boldsymbol{S} = \sum_{\boldsymbol{i}=\boldsymbol{1}}^{\boldsymbol{n}} \boldsymbol{wi} \,.\, \boldsymbol{xi} \qquad (3)$$

where:

– $\boldsymbol{S}$ is the total score (the value of the alternative against the criteria),

– $\boldsymbol{wi}$ is the weight of the criterion $\boldsymbol{i}$ (determines the importance of the criterion in the overall assessment),

– $\boldsymbol{xi}$ is the evaluation of the alternative against the criterion $\boldsymbol{i}$,

– $\boldsymbol{n}$ is the number of criteria.

Example:

Let's consider four criteria for evaluating an alternative in the context of military security (for example, for evaluating a military strategy or system):

1. Technologies (w1) – weight: 0.4
2. Resources (w2) – weight: 0.3
3. Adaptability (w3) – weight: 0.2
4. Coordination (w4) – weight: 0.1

Now let's set the assessments *xi* for each alternative against these criteria (on a scale of 0 to 10, where 10 is the highest score):

1. Technologies (x1): 8
2. Resources (x2): 6
3. Adaptability (x3): 7
4. Coordination (x4): 5

Calculation steps:

1. Multiply each weight $\boldsymbol{wi}$ by the corresponding value $\boldsymbol{xi}$.
2. Sum the results to get the total value $\boldsymbol{S}$.

The calculations are as follows:

S = (0.4×8)+(0.3×6)+(0.2×7)+(0.1×5)

S = 3.2 + 1.8 + 1.4 + 0.5

S = 6.9

The result of the overall security assessment "S" for this alternative is 6.9.

This indicates the overall effectiveness of the strategy or system in relation to the various criteria, with a higher number implying better performance against the listed criteria.

The first challenge that will shape the future dynamics of military security is the adoption and implementation of new technologies. It is one of the most important factors. Innovations in areas such as artificial intelligence, quantum computing, autonomous systems, space technology, and biotechnology are transforming traditional concepts of security while creating new risks and challenges.

The development of autonomous weapons systems, such as drones and autonomous platforms, is changing the nature of warfare, increasing its precision and reducing human risk. The threat of the use of unmanned aerial systems (UAS) in potential combat operations against both friendly and enemy forces is significant. [4]. At the same time, advances in cyber technology are leading to new forms of conflict, including cyberattacks on critical infrastructure, electronic networks, and financial systems. Space technologies, such as surveillance and communication satellites, provide strategic advantages but expand the battlefield with new opportunities for conflict.

New technologies are also significantly improving defense capabilities. Artificial intelligence and machine learning algorithms are helping to analyze large volumes of data, allowing for more accurate threat prediction and real-time decision-making. Advanced early warning systems based on quantum sensors and advanced radars are increasing the accuracy and range of potential risk detection.

Despite these opportunities, the adoption of new technologies comes with several challenges. Ethical and legal issues, such as the use of autonomous weapons or biotechnology for military purposes, raise serious concerns about the accountability and control of lethal technologies. Furthermore, the uneven distribution of access to these innovations exacerbates global imbalances, creating the conditions for asymmetric conflicts, while dual-use technologies, such as drones and cryptography, can easily be used for terrorist purposes.

Predictions about the impact of technology on military security range from optimistic to pessimistic. In the best-case scenario, technology can strengthen international cooperation through information-sharing platforms and joint defense systems, supported by ethical frameworks and international treaties that minimize the risk of abuse. In the worst-case scenario, however, new technologies can provoke arms races in new areas such as space and cyberspace, escalating conflicts and eroding trust between states.

To effectively manage the impact of new technologies, strategies such as investment in research and development to prevent technological monopolies, and the creation of international partnerships and regulations to control autonomous weapons and cyber technologies are needed. Resilient infrastructure, including secure networks and advanced crisis management systems, is also essential.

The conclusion is that new technologies offer enormous potential for improving defense capabilities, but their misuse or lack of effective control can lead to serious global threats. Effective prediction and management of technological innovations will play a key role in maintaining international stability and security.

The analysis shows that the scenario achieves an overall score of 7.2, highlighting its effectiveness, with the technology criterion contributing the most (0.5458). High values for technology and infrastructure highlight the importance of innovation and a stable supporting environment, while coordination and risk management remain areas for improvement. A strategic focus on the deployment of new technologies, combined with resilient infrastructure and international coordination, is key to addressing global challenges, but managing risks and strengthening cooperation between allies require additional efforts to achieve long-term stability.

The second challenge is hybrid warfare. It is a modern form of conflict that combines traditional military actions with unconventional means to achieve strategic goals. It combines elements such as cyberattacks, information operations, economic pressure, the use of mercenaries and terrorist networks, and the manipulation of political processes in opposing states. Hybrid warfare is difficult to predict and extremely effective in achieving asymmetric dominance. It is characterized by multidimensionality, including actions in land, sea, air, space, and cyber domains, as well as the use of economic sanctions, cultural and political pressures, and the manipulation of public opinion. Hybrid tactics are often used by weaker actors against stronger states or alliances, minimizing direct confrontation and relying on indirect methods. Moreover, these conflicts unfold without an official declaration of war, creating a *"gray zone"* in which it is difficult to identify the initiator of the attacks.

Key components of hybrid warfare are cyber operations targeting critical infrastructures such as energy networks, financial systems and communication channels, and cyber espionage to obtain strategic information. Information operations include the dissemination of disinformation, fake news and propaganda that destabilize the political environment and influence public attitudes through social media and controlled media channels. Political manipulation is expressed in support for movements or parties that can divide society or weaken state stability, as well as in undermining trust in democratic institutions through attacks on electoral processes. Economic pressure is applied through sanctions, trade blockades or control over energy resources, and illicit financial flows are used to destabilize the economic environment.

The impact of hybrid warfare on military security is significant. Difficulties in identifying threats and responsible actors make it difficult to formulate an adequate response, while at the same time strengthening the role of non-military means. Effective defense against hybrid attacks requires an integrated approach that includes diplomacy, economic strategies, and cyber defense. Traditional military forces must be complemented by new capabilities for information warfare, cyber defense, and societal resilience.

Countering hybrid threats requires strategies such as strengthening intelligence systems to identify early signs of hybrid attacks and establishing centers for analysis of disinformation and cyber threats. International cooperation is key to sharing information and resources, as well as developing regulations in the field of cyberspace and information security. The resilience of societies can be improved through educational campaigns that raise awareness of disinformation and through enhanced cybersecurity of critical infrastructure. Adaptive military strategies that integrate cyber capabilities and information operations are also crucial.

Hybrid warfare is one of the most complex aspects of modern military security, requiring innovative and adaptive approaches that combine traditional and non-traditional methods of defense. Success in managing hybrid threats depends on an integrated approach by states, effective international cooperation, and the resilience of societies against manipulation and pressure.

The overall score of 7.1 indicates that the strategy for addressing hybrid threats is effective, but with potential for improvement, especially in the areas of international cooperation and economic stability. To increase effectiveness, it is necessary to strengthen international cooperation through better coordination and resource sharing, increase information resilience by strengthening public awareness and improving educational campaigns, and improve economic stability through regulations against

illicit financial flows and building backup economic systems.

Next in line are **resilience and adaptabi**lity. They are key concepts for ensuring effective national and international security in a dynamic environment characterized by rapid change and emerging threats. They not only support protection against traditional and hybrid attacks, but also enhance the ability of states and organizations to respond adequately to unforeseen circumstances. Resilience is the ability of a system – whether military, economic or social – to maintain its functionality despite the impact of external shocks. It includes the protection of critical infrastructures such as energy networks, communication and transport systems by implementing backup mechanisms that ensure continuity of operations even in the event of disruptions caused by cyberattacks or physical destruction. Societal resilience is also essential, as it strengthens the preparedness and awareness of the population, increases trust in institutions and promotes social cohesion. In the digital era, cyber resilience is a fundamental component, including the protection of digital infrastructures, rapid recovery from cyberattacks and training of personnel to respond to critical situations.

The importance of resilience is expressed in its ability to minimize damage and ensure rapid recovery from crises, creating a basis for long-term security and stability. This problem did not arise suddenly, and leaders of European and world countries began discussing it several decades ago [5]. On the other hand, adaptability allows for effective coping with new and changing conditions, especially in the context of threats that do not follow traditional models. It includes flexibility of strategies, such as developing scenarios for action in different crises and using *"red teams"* to analyze vulnerabilities and propose innovative solutions. Training and development of military and civilian personnel, as well as the integration of technological innovations such as artificial intelligence and autonomous systems, are important aspects of adaptability. This ability promotes the efficient use of resources and provides a competitive advantage in a complex geopolitical environment.

The synergy between resilience and adaptability is crucial for predicting and managing military security. Resilience provides stability, while adaptability adds flexibility to deal with unforeseen situations. This combination allows for proactively addressing emerging threats, integrating lessons from past crises into future strategies, and strengthening cooperation between institutions, communities, and international partners.

However, several challenges make it difficult to implement resilience and adaptability. These include resource constraints that require significant investments in technology, training, and infrastructure, as well as the lack of effective coordination between different institutions and countries. The complexity of modern threats, such as cyberattacks and disinformation, also places new demands on the development of adequate solutions. Despite these challenges, resilience and adaptability remain fundamental pillars of modern military security, providing both stability in times of crisis and flexibility to respond to complex and rapidly changing threats. Their successful implementation requires coordinated efforts, innovation, and a deep understanding of global dynamics.

The overall score of 7.0 indicates that the resilience and adaptability system is well developed but with potential for improvement in the aspects of cyber resilience, strategy adaptability, and societal resilience. To increase effectiveness, additional investments are needed in protecting digital infrastructures and training personnel, improving strategic adaptability by developing scenarios for different threats and strengthening innovation, as well as measures to increase societal resilience through information campaigns and strengthening trust in institutions. This score highlights the importance of coordinated efforts and an integrated approach to addressing dynamic threats in the modern security environment.

Next in line is Multi-Domain Operations (MDO). They are an innovative and strategic approach to modern military security that responds to the complexity of the modern combat environment. They are based on integration and coordination between different domains – land, air, sea, space, cyberspace, and the information environment – to achieve operational superiority and effective management of resources and actions.

Multi-domain operations reflect the new reality of the global security environment, which includes non-traditional threats such as cyberattacks, disinformation, and hybrid warfare. At the same time, technological advances provide new tools for coordination, and geopolitical dynamics require adaptability and synchronization of efforts.

Cross-domain integration is at the heart of MDO, encompassing the synchronization of actions across domains to achieve operational objectives. The use of advanced technologies such as artificial intelligence, autonomous systems, and extended communication networks contributes to increased efficiency. Network-centric operations create globally connected networks to provide real-time information, facilitating decision-making through integrated data exchange. Flexible strategies allow for adaptation to changing conditions [6] and include a combination of offensive and defensive actions aimed at dominating key domains.

Multi-domain operations provide an operational advantage by accelerating decision-making processes through integrated command and control. They provide a better understanding of the operational environment through synergy between domains. Increased system resilience is achieved through the distribution of resources between domains and backup systems that ensure continuity in the event of failures. MDOs also introduce innovative tactics that include hybrid approaches such as disinformation and cyberattacks, as well as new technologies for dominating space and cyberspace.

Despite the many advantages, multi-domain operations face a number of challenges. Technological complexity requires significant investments in artificial intelligence, autonomous systems, and network connectivity, while vulnerability to cyberattacks and sabotage remains a serious threat. Coordination and integration across different units and domains can be hampered by the lack of unified protocols among allies. Legal and ethical issues are also significant factors, as the use of autonomous weapons and operations in space raises serious moral dilemmas, and the unpredictability of cyber operations can lead to the escalation of conflicts.

The future of MDO includes the integration of artificial intelligence, which will play a key role in data analysis and autonomous systems management. The development of space operations will be critical, including control of satellites and navigation systems and the introduction of new technologies for defense and attack in space. International cooperation will become even more important [7], requiring increased partnership between allies, sharing of resources, and common strategies to address global challenges.

Multi-domain operations offer a new approach to military security management in the context of rapidly changing threats and technologies. They require integration of resources, innovation, and global cooperation while offering the resilience and adaptability needed to cope with the complexity of the modern combat environment. Successful implementation of MDO will determine the ability of states and organizations to ensure their security in the future.

The overall score of 7.0 indicates that Multi-Domain Operations (MDO) is well-developed and effective, but there are areas for improvement, particularly in the use of technology and coordination between allies. To improve effectiveness, it is necessary to invest additional resources in technologies such as artificial intelligence and autonomous systems to increase operational effectiveness, improve coordination and management by developing unified protocols and data exchange between allies, and strengthen international cooperation by building joint strategies and sharing resources. These actions will support the sustainable development of MDO, ensuring the ability to address rapidly changing threats and technological challenges.

In fifth place are strategic alliances and partnerships. They are a fundamental element of the modern concept of military security in the global environment, which is characterized by geopolitical upheavals, technological innovations, and hybrid threats. Effective interaction between states, international organizations, and the private sector plays a key role in maintaining stability and building adaptive security systems.

The role of strategic alliances and partnerships includes stabilizing global and regional security by coordinating military efforts to ensure collective defense and response to threats. Allies create common prevention and response strategies aimed at traditional and non-traditional threats. In addition, resource sharing is achieved by sharing technology, infrastructure, and information, which reduces the individual burden on each country through coordinated financial and human resources. Strengthening interoperability is essential and includes the introduction of common standards and procedures that allow seamless interaction between different military forces, as well as the development of integrated command and control systems based on modern technologies.

Key forms of partnership include intergovernmental alliances such as NATO, which provides collective defense and adapts to new threats through programs such as NATO 2030 [8]. Bilateral and multilateral agreements also play a role in strengthening regional stability. Partnerships with international organizations such as the United Nations and the European Union are implemented to provide peacekeeping missions and conflict management, and participation in global initiatives such as the United Nations Sustainable Development Agenda is linked to addressing climate change as a factor for military security. Private-public partnerships include interaction with technology companies to develop innovations in defense and cybersecurity, creating common platforms for sharing information and raising awareness of threats.

The benefits of strategic alliances include increased readiness through faster response to crises and joint training programs and exercises that improve operational capabilities. The technological advantage provided through joint development and sharing of innovations contributes to strengthening cyber defense through globally coordinated efforts. The geopolitical influence of allies is also enhanced by countering the influence of hostile states through collective action.

Challenges facing strategic alliances include divergence of interests, as differences in national priorities and strategies can lead to internal tensions. Technological and operational differences also exist, as differences in the level of military technology development between allies and difficulties in integrating different platforms and systems can hinder effectiveness. Political instability in member states resulting from changes in political leadership can affect the stability of the alliance and increase the risks of termination of cooperation due to geopolitical pressures.

The future of strategic alliances is predicted to be digitalized and automated through the introduction of real-time data exchange platforms that improve joint planning and response. The use of artificial intelligence for threat analysis and coordination between partners will also play an important role. Expanding partnerships by integrating new members into existing alliances, especially in regions with increased risk of conflict, as well as strengthening cooperation with non-governmental organizations and civil society will be key to stability. Addressing global threats such as climate change, migration crises and hybrid threats will also require the creation of common strategies for cyber defense and the fight against disinformation.

Strategic alliances and partnerships are fundamental to anticipating and managing military security dynamics, providing a platform for collectively addressing the challenges of the modern security environment and strengthening the resilience and adaptive capacity of all participants. The success of these alliances depends on their flexibility, coordination, and ability to adapt to the ever-changing global context.

The overall score of 7.1 indicates that strategic alliances and partnerships have significant potential, but there are challenges related to geopolitical stability and coordination between partners. To increase their effectiveness, it is necessary to reduce the differences in interests and strategies between partners, in order to improve internal coordination and reduce internal tensions. It is also necessary to strengthen the integration of new technologies, such as artificial intelligence and automation, to modernize military systems and improve cyber defense. Strengthening global stability through better geopolitical coordination and active participation in international initiatives to address emerging global threats is of key importance. These actions will increase the effectiveness and adaptability of alliances, ensuring stability and preparedness for future challenges.

Based on the calculations and analysis using Saati's method, **the adoption and implementation of new technologies** in the biggest challenge that determines the future dynamics of military security. The reasons behind this are:

1. **Technological complexity and speed of innovation:** Rapid advances in technologies such as artificial intelligence, quantum computing, and autonomous systems require significant investment, expertise, and time for integration. Military organizations often lag behind the private sector in developing and implementing innovations.

2. **Cybersecurity and vulnerabilities:** New technologies bring with them an increased risk of cyberattacks. Devices and systems based on artificial intelligence or connected via IoT are particularly vulnerable to sabotage, espionage, and manipulation.

3. **Financial constraints:** Implementing advanced technologies requires huge financial resources for research, testing, maintenance, and staff training. For many countries, these costs are difficult to justify, especially with limited budgets.

4. **Operational integration:** Incorporating new technologies requires adapting existing platforms, procedures, and organizational structures. The lack of standards and interoperability among allies further complicates the process.

CONCLUSIONS

The diagram visualizes the challenges to military security, with the weights of the factors presented in percentages for clarity. The highest weight is given to the adoption and implementation of new technologies (30%), which highlights their key role. Strategic alliances and partnerships (25%) also occupy a significant place, highlighting their impact on stability and effectiveness. Resilience and adaptability (20%) complement the basic requirements for dealing with the dynamic environment. Multi-domain operations (15%) and hybrid warfare (10%) have lower, but still important, weights. The main conclusion is that the strategic focus should be on new technologies and alliances, as they combine innovation and coordinated efforts to address modern challenges.

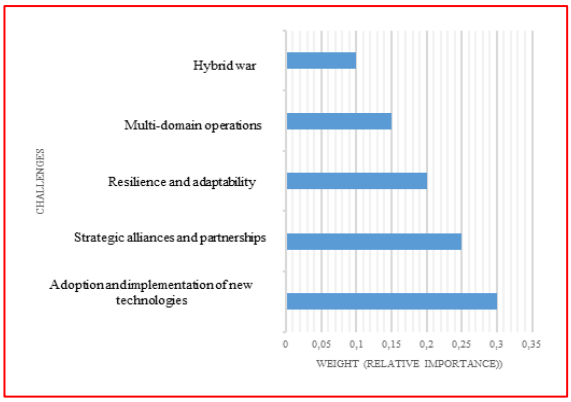


Fig. 2. Comparison of military security challenges.

The conclusion from examining the dynamics of military security in the context of global (in)security is that the future state of military security will be shaped by the ability of states to adapt to the constantly changing environment. Despite growing global threats, such as hybrid conflicts, cyberattacks, and emerging technological risks, there are significant opportunities to strengthen military security through innovation and strategic cooperation. Key factors that will shape the future of military security include the integration of new technologies, a proactive approach to hybrid threats, the development of adaptive and multi-domain systems, as well as strengthening of international cooperation and alliances. The successful integration of these elements will require not only technical and operational readiness but also ethical and legal awareness of new challenges, which will allow for the sustainable formation of stable strategic approaches in the context of global uncertainty.

ACKNOWLEDGMENTS

This report is supported by the National Science Program Security and Defense, approved by decision No. 171/21.10.2021 of the Council of Ministers of the Republic of Bulgaria.

REFERENCES

[1] V. Statev, Does combat deployment experience affect the commander's decision-making process?. Environment. Technology. Resources. Proceedings of the 15th International Scientific and Practical Conference. Volume IV. Rezekne, Latvia, 2024. pp. 251-254.

[2] N.Nichev, K. Koynakov, Use of unmanned aircraft in the logistics support of military formations. The Eurasia Proceedings of

Science, Technology, Engineering & Mathematics (EPSTEM), 2024, pp. 92-99.
[3] K. Koynakov, Logistical reconnaissance using unmanned aerial vehicles. Proceedings of the scientific conference “Logistics and social systems”. 2021, pp.76-84.
[4] N.Tsvyatkov, System for countering unmanned aerial systems – threat analysis and force protection planning, NMU Annual University Scientific Conference, 2024, pp. 433-443.
[5] N. Dolchinkov, N. Nichev, Gamma-background radiation control systems as a factor of Bulgaria's national security, Environment. Technology. Resources. Rezekne, Latvia, Proceedings of the 15th International Scientific and Practical Conference. Volume IV, pp 83-88.
[6] N. Dolchinkov, Optimizing energy efficiency in the conditions of a global energy crisis, Optimizing Energy Efficiency During a Global Energy Crisis, 2023, pp. 1-9.
[7] S. Stoykov, Risk management as a strategic management element in the security system, International Conference on Creative Business for Smart and Sustainable Growth, CreBUS 2019, March 2019, Article number 8840098, Category number CFP19U17-ART; Code 152084, pp. 156-160.
[8] S.Stoykov, The system of education, training and research in the field of security - managing change through experience and knowledge, ETR, vol. 4, 2024, pp. 269-274.
[9] Nato, [Online]. Available: https://www.nato.int/nato2030/ [Accessed: Feb. 18, 2025].

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference, 2025. Volume V, 171-178

Collective Defense – a Means to Achieve a More Sustainable Future

Rumen Marinov
Security and Defense Faculty
Vasil Levski National Military University
Veliko Tarnovo, Republic of Bulgaria
ramarinoff@gmail.com

***Abstract* — The report analyzes the geopolitical situation in the world at the beginning of 2025. NATO is entering its eighth decade as a successful military-political alliance but faces new threats, which we will examine in this study. The conflict between Russia and Ukraine highlights the need for adaptation, deterrence, and innovation. NATO's Strategic Concept until 2022 reaffirms its commitment to unity and security. This study uses the Thomas L. Saati and Lotka–Volterra equations for security analysis, identifying key dependencies in the changing landscape. It outlines five main challenges: adapting NATO and the EU to new threats, modernizing military systems, prioritizing military security in Bulgaria, increasing the military budget by 2027, and emphasizing collective defense for European resilience. An interdisciplinary approach is crucial to address these challenges effectively.**

Keywords – Geopolitics, Security, NATO, Adaptation, Military Resilience

I. INTRODUCTION

NATO is entering its eighth decade as a successful military-political alliance, covering a significant share of the world's GDP and population, but facing a growing range of threats and challenges. The changing geopolitical environment, including the rise of revisionist authoritarian states, hybrid threats, terrorism, and new technologies, requires the alliance to continue adapting while maintaining its cohesion and strengthening its military and political mechanisms.

The reseach aims to analyze the geopolitical situation in early 2025, focusing on the new threats and challenges facing NATO and the EU in the context of the changing international environment. The aim is to identify key dependencies and strategic directions for adaptation, deterrence, and innovation through an interdisciplinary approach, including the equations of Thomas L. Saatchi and Lotka-Volterra. The study sets out to outline five main security challenges, including: the adaptation of NATO and the EU to new risks, the modernization of military systems, the prioritization of military security in Bulgaria, the increase in the military budget by 2027, and the strengthening of collective defense to strengthen European resilience.

II. MATERIALS AND METHODS

The study uses combined methods to analyze military security in the contemporary global context. It conducts a literature review of theoretical and empirical sources, examines documents and strategic reports of governmental and international organizations, and provides examples of emerging threats through case studies and comparative analyses of strategies of different countries and organizations.

III. RESULTS AND DISCUSSION

After the start of the military conflict (special military operation) between Russia and Ukraine in 2022, the need to rethink national and collective security has intensified. The environment in which the armed forces operate increases the number of its components as technology develops and new tactics are applied [1]. In response to these dynamics, NATO focuses on strategic adaptation, strengthening deterrence, technological innovation, and resilience to climate and pandemic threats. A key focus is on preserving collective defense, democratic principles, and the rules-based international order.

NATO's 2022 Strategic Concept reaffirms the commitment to unity, security, and cooperation. The changing security environment is increasingly bringing to

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8493
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

the fore the risks of radicalization of large societal groups and related acts of violence motivated by extremism and terrorism [2].

This means that national security systems must face this risk and create the necessary regulatory, financial, informational, and human capacity for early warning, prevention, response, counteraction, and effective management of its consequences [3].

In parallel, the European Union defined its "Strategic Compass" for security, aiming to improve capabilities for joint response to threats, including through investments in technology and partnerships.

Military security is a key factor in a dynamic security environment that requires synchronization between military and political mechanisms to effectively address threats. According to the Marshall publication, "A dynamic security environment is constantly changing and evolving, requiring security measures to be constantly updated and adapted to keep pace with new threats and risks [4].

Significant and dynamic changes in the strategic security environment require adaptation and transformation of security and defense systems in the real global and regional environment [5]. It can be argued that the dynamic security environment requires organizations and individuals to be highly adaptable and operationally flexible. This adaptability must be supported by a strategic focus on continuous learning and improvement to anticipate and effectively manage emerging risks and threats. A key role in this process is played by broad expertise in the field of safety and security, which provides the basis for integrated and sustainable solutions. Some specialists pay particular attention to the determinants of internal and external influence on security [6]. The more dynamic the security environment, the more critical the ability to absorb and improve resilience becomes. In this context, the resilience aspects of management systems are considered comprehensive and also include elements of human resource management, organizational design, and crisis management [7]. The role of NATO and the European Union in the context of military security is crucial for stability and resilience in a context of increasing uncertainty. NATO is strengthening collective defense by investing in technology, strengthening strategic deterrence against revisionist states, and upholding democratic values. In parallel, the EU Strategic Compass complements these efforts with a focus on autonomous crisis response, partnerships to maintain international order, and the synchronization of military and civil security. The conflict in Ukraine highlights the importance of flexible mechanisms to address hybrid threats, modernizing military structures, and investing in technologies that provide an advantage on the battlefield and in cyberspace. Military security remains the basis for collective defense, integrating adaptation to new risks and the promotion of shared values and international cooperation.

The NATO-EU relationship has taken on even greater importance in light of the dramatic shift in the security environment since 24 February 2022, when the conflict between Russia and Ukraine has intensified the need for transformation in both national and international security strategies. The dynamics of "Military Security" have gained greater focus in response to this sharp shift in the security environment, especially in the context of the military conflict between Russia and Ukraine. This profound shift in the security context and emerging threats necessitates a reassessment of the relative importance of a country's national security subsystems.



Fig. 1 The key aspects of the role of NATO, the EU, and the impact of the conflict in Ukraine in the context of military security.

The study continues by applying Saati's methodology, which provides a systematic approach to analyzing and prioritizing security subsystems adapted to the specific needs of a given situation. In addition, predictions made using the Lotka-Voltaire and Kolmogorov methods contribute to a more precise ranking of these subsystems in terms of importance, taking into account the interactions between different factors. This assessment reveals deeper dependencies within the dynamically changing military security, in which technological progress, geopolitical dynamics, emerging threats, and societal changes are asserting themselves as critical elements for adapting and strengthening national and collective security.

Based on the performed analysis [8] we can conclude that military security [9] takes a central place in the national security system of Bulgaria [10], and its importance is confirmed by using Saati's method of hierarchy analysis. This approach reveals that military security, along with economic and demographic security, are priority subsystems necessary to ensure resilience and adaptation in a changing geopolitical environment. The study emphasizes the importance of clear hierarchies and interaction between subsystems for effective security management. Hierarchy of national security subsystems depending on the force majeure change in the security environment of the Balkan Peninsula, from 24.02.2022 to 01.06.2022 military conflict between Russia and Ukraine (variant). Their hierarchy is presented in Table 1 and Fig. 2.

Regression equation:

$$y = 0{,}0001x^4 - 0{,}0031x^3 + 0{,}0233x^2 - 0{,}0779x + 0{,}2137$$

Coefficient of determination: $R^2 = 0{,}5798$

In this case, which means that about 57.98% of the variation in y can be explained by this equation. This is considered a medium-strong relationship.

TABLE 1

security subsystems	coefficient	security subsystems	coefficient
A1- Military security	0,157	A7- Ethnic security	0,029
A2 - Economic security	0,115	A8- Energy security	0,027
A3 - Geostrategic security	0,134	A9- Migration security	0,097
A4 - Demographic security	0,132	A10- Cyber security	0,007
A5 - Information security	0,047	A11- Environmental security	0,001
A6 - Food security	0,133	A12- Health security	0,121
Total		1	

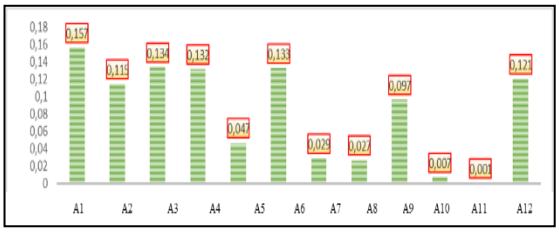


Fig. 2 Hierarchy of national security subsystems from 24.02.2022 to 01/06/2022 – military conflict between Russia and Ukraine

The data presented in Table 1 regarding the priority of the subsystems of national security in a force majeure situation show that at this particular moment "Military Security" – takes the first place with a relative weight of 0.157. This is thanks to the membership of the Republic of Bulgaria in the collective defense of NATO. Economic security takes second place due to the geographical location of the country and its membership in NATO. The remaining subsystems, such as Geostrategic Security and Demographic Security, necessarily follow the first two subsystems due to their close connection and mutual dependence, Fig. 2.

The force majeure situation led to a significant change in the security environment on the Balkan Peninsula. This development is due to the interaction of at least two different factors, which subsequently led to a reconfiguration of the hierarchy between the security subsystems, an integral part of the national security of the Republic of Bulgaria.

Changing the level of threat on the Balkan Peninsula, due to the simultaneous actions of two or more reasons, implies the complex accounting, arrangement, and influence of the subsystems that are part of the country's national security. A similar situation was observed in the second half of 2022, where the state of national security will be determined both by the increased probability of an escalating military conflict between Russia and Ukraine, as well as by the existing health pandemic, increased migration coming from the Republic of Turkey, and of course by growing inflation. In the security environment so formally described, using the well-known Saati methodology, a hierarchy of importance in the specific situation of the security subsystems is obtained. Their complex influence in sequence is presented in Table 2 and Fig. 3

The hierarchy of national security subsystems depends on the complex change in the security environment on the Balkan Peninsula and the world from 01.06.2022 to the end of 2022 in combination with a projected escalating military conflict between Russia and Ukraine and a subsiding health pandemic, economic reasons, and migration (variant).

TABLE 2

security subsystems	coefficient	security subsystems	coefficient
A1- Military security	0,187	A7- Ethnic security	0,029
A2 - Economic security	0,116	A8- Energy security	0,034
A3 - Geostrategic security	0,154	A9- Migration security	0,11
A4 - Demographic security	0,112	A10- Cyber security	0,007
A5 - Information security	0,048	A11- Environmental security	0,001
A6 - Food security	0,113	A12- Health security	0,089
Total			1

Regression equation:

$$y = 4E - 0{,}5x^5 - 0{,}0011x^4 + 0{,}0123x^3 - 0{,}0555x^2 + 0{,}0777x + 0{,}1415$$

Coefficient of determination: $R^2 = 0{,}6552$

In this case, which means that about 65.52% of the variation in y can be explained by this equation. This is considered a medium-strong relationship.

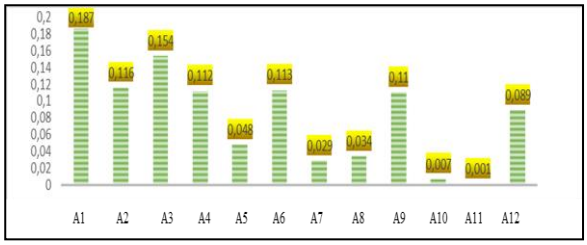


Fig. 3 Hierarchy of national security subsystems in the second half of 2022 - from 01.06.2022 to the end of 2022 - the military conflict between Russia and Ukraine, migration, and economic reasons

The results presented in Fig. 3 are obtained according to the criteria taking into account the importance of both reasons for the change in the state of the security environment. In this case, the resulting hierarchy for the first reason, for example, an escalating military conflict between Russia and Ukraine and a subsiding health

pandemic, economic reasons, and migration, "Military Security" dominates over the others with a relative weight of 0.187 or 18.7%. The remaining "Economic Security" and "Geostrategic Security" in terms of importance, as well as the minimum values of "Health Security" fully correspond to the logic. The philosophy of the response of the national security system to reduce the consequences of the threat to the country, Fig. 3.

The hierarchy of the national security subsystems in the security environment of the Balkan Peninsula and the world (variant) for the period from 01.01.2023 to 01.06.2023 is presented in Fig. 4.

TABLE 3

security subsystems	coefficient	security subsystems	coefficient
A1- Military security	0,229	A7- Ethnic security	0,039
A2 - Economic security	0,128	A8- Energy security	0,032
A3 - Geostrategic security	0,154	A9- Migration security	0,121
A4 - Demographic security	0,108	A10- Cyber security	0,006
A5 - Information security	0,046	A11- Environmental security	0,012
A6 - Food security	0,103	A12- Health security	0,022
Total			1

Regression equation: $y = 4E - 0{,}5x^4 - 0{,}0015x^3 + 0{,}0185x^2 - 0{,}1066x + 0{,}3104$

Coefficient of determination: $R^2 = 0{,}7593$

In this case, which means that about 75.93% of the variation in y can be explained by this equation. This is considered a strong relationship.

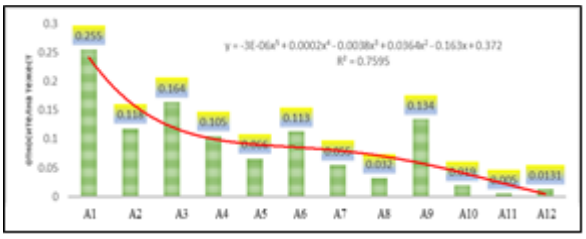


Fig. 4 Hierarchy of national security subsystems from 01.01.2023 to 01.06.2023 - the military conflict between Russia and Ukraine remains

In the specified period, the subsystem "Military Security" is again in a priority position with a relative weight of 0.209, which constitutes almost 21% of the value of the national security system of the country taken as 100%. In the general trend of development of the security environment, mainly expanding military conflicts - Russia Ukraine, Syria, Israel in the Gaza enclave and the tension between Kosovo and Serbia, it is quite normal for "Economic Security" and "Geostrategic Security" to occupy second and third place in the security system in the country, Fig.4.

The hierarchy of national security subsystems in the security environment of the Balkan Peninsula and the world (option) for the period from 01.06.2023 to 31.12.2023 remains.

TABLE 4

security subsystems	coefficient	security subsystems	coefficient
A1- Military security	0,229	A7- Ethnic security	0,039
A2 - Economic security	0,128	A8- Energy security	0,032
A3 - Geostrategic security	0,154	A9- Migration security	0,121
A4 - Demographic security	0,108	A10- Cyber security	0,006
A5 - Information security	0,046	A11- Environmental security	0,012
A6 - Food security	0,103	A12- Health security	0,022
Total			1

Regression equation: $y = 1E - 0{,}5x^5 - 0{,}0004x^4 + 0{,}0035x^3 - 0{,}0073x^2 - 0{,}0502x + 0{,}2724$

Coefficient of determination: $R^2 = 0{,}7616$

In this case, which means that about 76.16% of the variation in y can be explained by this equation. This is considered a strong relationship.

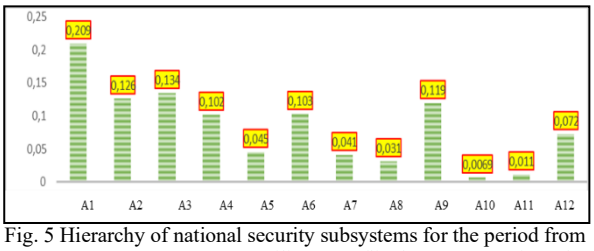


Fig. 5 Hierarchy of national security subsystems for the period from 01.06.2023 to 31.12.2023 - military conflict between Russia and Ukraine

TABLE 5

security subsystems	coefficient	security subsystems	coefficient
A1- Military security	**0.241**	A7- Ethnic security	**0.055**
A2 - Economic security	**0.138**	A8- Energy security	**0.032**
A3 - Geostrategic security	**0.164**	A9- Migration security	**0.134**
A4 - Demographic security	**0.108**	A10- Cyber security	**0.019**
A5 - Information security	**0.066**	A11- Environmental security	**0.012**
A6 - Food security	**0.118**	A12- Health security	**0.021**
Total			1

The changes in the hierarchy of security subsystems are presented in Fig. 6:

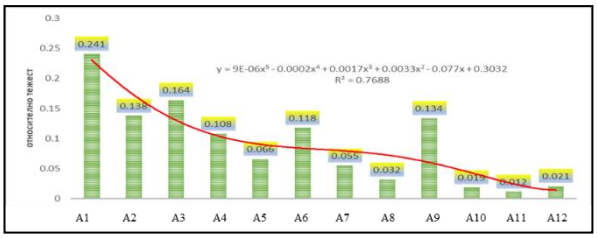


Fig. 6. Hierarchy of national security subsystems for the period from 01.01.2024 to 01.06.2024 - military conflict between Russia and Ukraine

TABLE 6

security subsystems	coefficient	security subsystems	coefficient
A1- Military security	**0.255**	A7- Ethnic security	**0.055**
A2 - Economic security	**0.118**	A8- Energy security	**0.032**
A3 - Geostrategic security	**0.164**	A9- Migration security	**0.134**
A4 - Demographic security	**0.105**	A10- Cyber security	**0.019**
A5 - Information security	**0.066**	A11- Environmental security	**0.005**
A6 - Food security	**0.113**	A12- Health security	**0.0131**
Total			**1**

Regression equation: $y = -0{,}0157x^4 + 0{,}2268x^3 - 0{,}2664x^2 - 4.609x + 23.528$

Coefficient of determination: $R^2 = 0{,}9605$

In this case, which means that about 96.05% of the variation in y can be explained by this equation. This is considered a strong relationship.

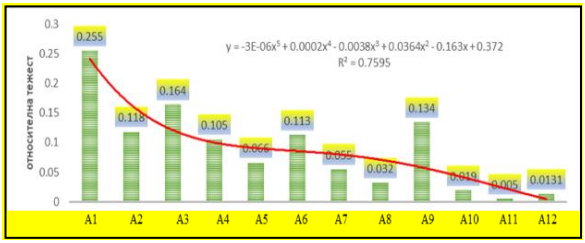


Fig. 7 Hierarchy of national security subsystems for the period from 01.06.2024 to 01.12.2024 – military conflict between Russia and Ukraine

The analysis shows that the simultaneous consideration of two or more reasons that shape the change in the state of the security environment in a given region implies a dynamic and adequate change (relative weight of influence) specifically for "Military Security" in the composition of the country's national security. Furthermore, when considering the place of this security subsystem, its dynamics must always be considered no less than the simultaneous action of at least two or more reasons that shape the state of the Security Environment. Research shows that with these and other changes in the security environment, the "Military Security" subsystem is always in the top three places in terms of importance for the functioning of the country's national security system, Table 6 and Fig. 7.

The relative weight of influence of the "Military Security" subsystem in relation to the National Security system depends on the complex change in the security environment on the Balkan Peninsula and in the world, from March 13, 2020, to December 31, 2024, in the Security Environment formed for the period mainly: the Covid 19 pandemic, escalating military conflict between Russia and Ukraine, military actions between Israel and Hamas in the Gaza Strip, refugee migration, inflation, etc. The indicated military-political situation in the world and the Balkan Peninsula, the relative weight of influence of the "Military Security" subsystem in relation to the National Security system is presented in Table 7.

The relative weight of influence of the Military Security subsystem relative to the National Security system

TABLE 7

Periods for analysis of national security - military security	Relative weight of military security by periods – percentages
until March 13, 2020	***19.1***
after March 13th until July 2020	***13.8***
from July 15 to the end of December 2020	***13.5***
beginning of 2021 until July 1, 2021	***11.3***
from July 1 to February 24, 2022	***11***
from 24.02.2022 to 01.06.2022	***15.7***
from 01.06.2022 until the end of 2022	***18.7***
from 01.01.2023 to 01.06.2023	***20,9***
from 01.06.2023 to 31.12.2023	***22.9***
from 01.01.2024 TO 01.06.2024	***24.1***
from 01.06.2024 TO 31.12.2024	***25.5***

The indicated values of the relative weight of influence of the "Military Security" subsystem in relation to the National Security system are presented in Fig.8.

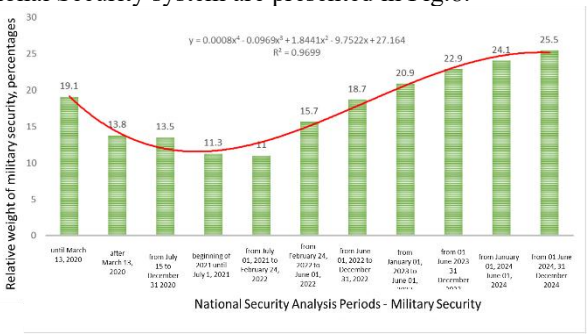


Fig. 8. Relative weight of the "Military Security" subsystem to National Security in the country in percentages for the periods from March 13, 2020, to December 31, 2024.

The interdependence by periods of national security analysis and their respective relative weights (Fig. 8.) form a regression equation as shown:

$$y = 0.008x^4 - 0.0969x^3 + 1.8441x^2 - 9.7522x + 27.164$$

Coefficient of determination: $R^2 = 0.9699$

The equation shows how the importance of different time periods for national security changes with very high accuracy. Such analysis is useful for strategic planning, as it highlights which periods were most important and can help predict future trends.

The changes in the values of the relative weights of the subsystem "Military Security", are presented in Table 7. The period from March 13, 2020, to 31.12.2023, demonstrates that the minimum value of 0.11 or 11% is observed in the segment from July 1 to February 24, 2022, Fig. 8. Minimum values of the subsystem "Military Security" are observed in the period - after March 13, 2020. to July 2020. and from June 1, 2022. to the end of 2022. This is mainly due to the priority relative values of the subsystem "Health Security" - due to the "Covid 19" pandemic in values from 13.8 to 18.7 percent, Fig. 8. The increase in the relative values of the "Military Security" subsystem is observed throughout 2023, where it increases in relative values, respectively - in the first part of the year 20.9 to 22.9 percent in the second. The derived regression dependence based on the relative values of the "Military Security" subsystem for the specified period from March 13, 2020, to December 31, 2024, is characterized by a concordance coefficient R2=0.9699 or almost 97% of the changes during the period can be expressed, described with this regression equation presented in Fig. 8.

Important for the study is the dynamics of the subsystem "Military Security" in the changing security environment, which is the possibility of predicting the nature of its change in a close, immediate period of time, for example, 6 months. For this purpose, a forecast was made by the relative weight of the subsystem "Military Security" based on the latest data for 2023. A forecast in relative weight of the influence of the subsystem "Military Security" depending on the complex change in the security environment on the Balkan Peninsula and in the world for the period from 01.01.2024 to 01.06.2024 in a situation of escalating military conflict between Russia and Ukraine, events in the Middle East - Israel, Palestine, Syria refugees and emerging inflation (variant), is presented in Fig. 9.

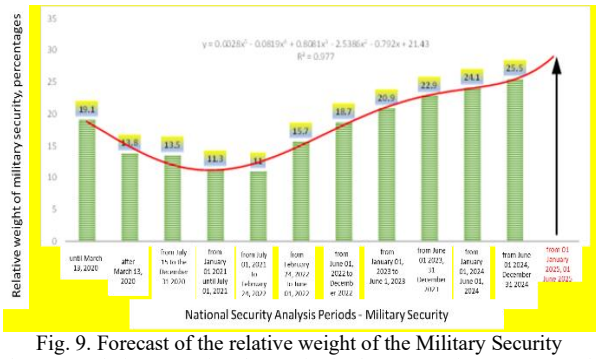


Fig. 9. Forecast of the relative weight of the Military Security subsystem relative to National Security in the country in percentages for the first half of 2025

The results of the forecast demonstrate that by 01.06.2025 the relative weight of "Military Security" will increase to 24.9% or almost 25%. This value requires significant funding through an increase in the military budget for this and next year. Of particular scientific interest are the reaction time, the reflection of the "Military Security" subsystem in relation to the dynamics of development, and changes in the security environment for the period from 24.02.2022 to 31.12.2024.

Using the modified Lotka-Voltaire model for military security analysis for the period from 24 February 2022 to 31 December 2024.

The Lotka-Voltaire model is a mathematical framework used to describe the population dynamics of predators and prey. The model assumes that the growth of the predator population depends on the availability of prey, while the growth of the prey population depends on the number of predators. This relationship leads to complex dynamics characterized by cyclical fluctuations in the size of both populations.

Applying this model to military security, we can consider the predator population as a country's military forces and the prey population as the civilian population. In this context, the growth of military forces depends on the availability of resources (civilian population), while the growth of the civilian population depends on the size of the military forces.

The modified Lotka-Volter model can be represented by the following differential equations, where:

$$\frac{dN}{dt} = rN - aNP \qquad (1)$$

$$\frac{dP}{dt} = bNP - cP \qquad (2)$$

– "N" represents the population of the "predator" (military forces, changing security environment);

– "P" represents the "prey" population (Military Security);

– "r" and c are natural growth rates respectively for N and P;

– "a" and b are interaction coefficients between "N" and "P".

By solving these equations, we can obtain the dynamics of the populations of "predators" ("External Security Environment") and "prey" ("Military Security"). This allows us to analyze the impact of various factors on the "Military Security" of the country, such as changes in resources, technological progress of the entities forming the "External Security Environment" or their external change.

When taking into account the average values of the changes in the "Security Environment", the reaction of the "Military Security" subsystem according to the Lotka-Voltaire method. Especially in the method, it represents the reaction time, the dynamics of change, of the "Military Security" subsystem to changes in the "Security Environment". For example, for the period from February

24, 2022, to December 31, 2024, the reaction time to changes in the “Military Security” subsystem is presented in Fig. 10.

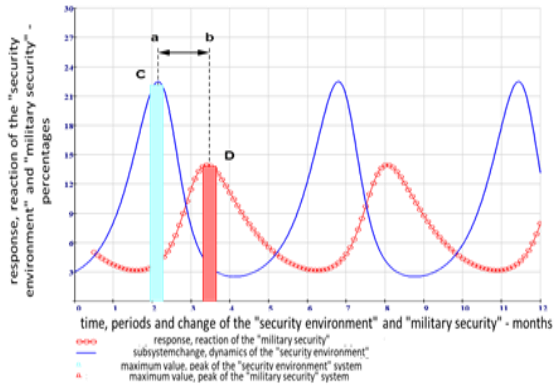


Fig. 10. Dynamics of the security environment according to the Lotka-Voltaire method for the period from February 24, 2022, to December 31, 2024

The response time of the security environment, especially in the current military conflicts near our country - the escalation of the war in Ukraine, the events in the Middle East - Israel, Palestine, Syria, inflation, impoverishment, etc. presented in Fig. 10. demonstrates a peak in the changes of the “Security Environment”. For example, point “C” reaches the maximum of the changes of the "Security Environment", with an average value of 22% (from 3 to 22 percent) And the maximum of the response, the reaction of the subsystem "Military Security", the maximum - point “D” has an average value of 14%. On this occasion, the response time of the subsystem "Military Security" for the period 24.02.2022 - 31.12.2024 is from 30 to 45 days shown between points “a-b”, Fig. 10. This period includes only the reaction of the country's management units for managing the values of the security subsystems when the “Security Environment” changes.

In the rapidly evolving global and regional security environment, military security faces complex and multifaceted challenges. To address them, it is necessary to develop and implement an integrated and proactive strategy. Its main components include the implementation of technological innovations, adaptation to hybrid and multi-domain threats, strengthening strategic partnerships, and compliance with ethical and legal standards. The entire European community aspires to promote partnership and unity among all EU member states. [11]

The systematic approach to military security management provides the opportunity for long-term forecasting (within 3-7 years), while identifying investment priorities and ensuring effective resource allocation. The analysis and assessment methodology is aimed at a smooth transition to higher levels of security through an in-depth consideration of the factors affecting military stability. This is especially important in the context of increasing geopolitical instability in the Balkan region, where a synergistic approach is crucial to strengthening resilience. These management challenges increase significantly in the context of finding effective solutions in the balanced role of human capital in organizations. [12]

The strategies and payment matrix for ensuring Bulgaria's national and military security focus primarily on the acquisition of high-tech weapons systems and the increase in the military budget. This strategic direction emphasizes Bulgaria's commitment to building a stable military force capable of maintaining security and stability on the Balkan Peninsula.

The continuous implementation of the strategies and payment matrix for ensuring the national and military security of the country by the leadership contributes to establishing a sustainable dynamic in the growth of military security and the protection of national interests, which is of crucial importance for the field of regional and collective security. The development of technologies will be one of the few positive long-term consequences of the crisis. [13] Digital transformation requires significant investments, technological innovations, and targeted measures to stimulate digital competence and digital culture.[14]

IV. CONCLUSIONS

This study offers new perspectives on collective defense and highlights the need for an interdisciplinary approach to more effectively address the related challenges. These challenges can be categorized into five key areas. The first key area, NATO and the EU are adapting to emerging threats, focusing on strategic deterrence and enhanced cooperation between allies in light of the Russia-Ukraine conflict. The second, the changing global security landscape requires the modernization of military systems and an emphasis on strengthening cybersecurity, especially in response to the ongoing conflict in Ukraine and rising regional tensions in the Balkans. The security environment is influenced by the risks and challenges of the conflicts in the country and in the countries close to the Republic of Bulgaria [15].

The third key area, Bulgaria faces an imperative to prioritize military security in the post-2022 security environment, which requires increased investment in defense capabilities, even as a NATO member. Fourth, by 2027, military security is expected to comprise 25.5% of Bulgaria’s national security framework, which highlights the need for a larger military budget and innovative strategies to counter hybrid threats and cyberattacks. Finally, the fifth key area, the principle of collective defense, is crucial for the resilience of both Bulgaria and Europe, which requires coordinated strategies and investments in modern defense technologies by both NATO and the EU.

REFERENCES

[1] D. Ivanov, The Nuclear family in Modern terrorism, Proceedings of the 15th International Scientific and Practical Conference, June 27th-28th, 2024, Latvia. Rezekne, Rezekne Academy of Technologies, 2024.

[2] P. Marinov, L. Milushev and D. Ivanov, Security in Bulgaria through the prism of contemporary challenges and threats,

Proceedings of a scientific conference - Current security issues, Volume I, Veliko Tarnovo, Bulgaria. Vasil Levski National Military University, 2023.

[3] V. Statev, The Systems Approach: a Small Tactical Unit, Security Horizons, Volume III, No. 6. Skopje, North Macedonia, 2022.

[4] V. Vasilev, D. Stefanova and C. Popescu, Human capital management and digitalization-from good practices and traditions to sustainable development, Book Chapter*:* Digitalization, Sustainable Development, and Industry 5.0: An Organizational Model for Twin Transitions, 2023.

[5] V. Vasilev, D. Stefanova and M. Icheva, Green human resource management as a component of sustainable organizational development in environmental and natural economics, Proceedings of the 15th International Scientific and Practical Conference, June 27th-28th, 2024, Latvia. Rezekne, Rezekne Academy of Technologies, 2024.

[6] K.Krastev, Determinant Analysis of External Influence on the Bulgarian National Security Policy, The 22nd International Scientific Conference Knowledge-Based Organization, Sibiu, Romania, vol.I, 2016

[7] Strategic security environment and the role of military engineering support in operations", HORIZONS INTERNATIONAL SCIENTIFIC JOURNAL Series A, Social Sciences and Humanities, Year XIV, Volume 29, December 2021

[8] N. Nikolova, Human capital in the changing work environment of industry 4.0, Proceedings of the 15th International Scientific and Practical Conference, June 15th-16th, 2023, Latvia. Rezekne, Rezekne Academy of Technologies, 2023.

[9] N. Nikolova, Industry 4.0 - development and consequences for sustainable development of Bulgaria, Proceedings of the 15th International Scientific and Practical Conference, June 15th-16th, 2023, Latvia. Rezekne, Rezekne Academy of Technologies, 2023.

[10] N. Nikolova, Development of a System for Assessment of Digital Professional Suitability in the Company Environment, Proceedings of the 15th International Scientific and Practical Conference, June 15th-16th, 2023, Latvia. Rezekne, Rezekne Academy of Technologies, 2023.

[11] S. Stoyko, Scientific Knowledge - Source of a Competitive Advantage in Security, Published in International Conference on High Technology for Sustainable Development (HiTech), 11-14 June 2018, Sofia, Bulgaria, 2018.

[12] N. I. Padarev, Application of Software Platforms to Enhance Early Warning and Detection System Capabilities for Nuclear Weapons, Proceedings of the 15th International Scientific and Practical Conference, June 27th-28th, 2024, Latvia. Rezekne, Rezekne Academy of Technologies, 2024.

[13] A. White, „Report on EU-NATO cooperation in the context of transatlantic relations", June 2021, [Online]. Available: https://www.europarl.europa.eu/doceo/document/A-9-2021-0192_BG.html?utm_source=chatgpt.com [Accessed: Apr. 21, 2025].

[14] Publications Office of the European Union. Responsible entity(ies): European External Action ServiceJune 2021, [Online]. Available: https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=LEGISSUM:collective_defence [Accessed: Apr. 21, 2025].

[15] D. Palmer, Rachael Gosnel, An Evolution in Arctic Collective Defense, November 2024. [Online]. Available: https://www.thearcticinstitute.org/evolution-arctic-collective-defense/ [Accessed: Jan. 05, 2025].

[16] S. Ashbridge, A. Beard, Greening Defence: Prioritising Climate Change for a Sustainable Future, January 202. [Online]. Available: https://rusi.org/explore-our-research/publications/commentary/greening-defence-prioritising-climate-change-sustainable-future [Accessed: Jan. 07, 2025].

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 179-183

A Change in the Way Artillery is Used, Based on the Russia-Ukraine Conflict

Dilyan Markov
Rakovski National Defence College
Sofia, Bulgaria
dilyanmarkov@abv.bg

Abstract— Artillery for the execution of firing tasks is deployed in a battle order, which from a long time ago was aimed at massed fire and hitting targets with the use of a large amount of ammunition from the force for artillery support. Different configurations were applied to the means of defeat, depending on the probable threats and countermeasures against the artillery during the period of time that can be specified as expired. This tactic is also used in the initial phase by both sides of the conflict between Russia and Ukraine since 2022.

The introduction of new means of countermeasures against artillery systems and the improvement of existing ones impose changes on the battlefield, concerning the determination of data for firing per hit and the number of guns used.

One of the important elements affecting this is the time, both for preparation and for staying at firing positions on the guns. No less important is the amount of artillery systems used, which practice shows that reduced to one or two units from batteries and divisions used in the past, gives the desired effect, combined with improved accuracy of fire and increased survivability on the battlefield for artillery.

The combination of all this with a timely and covert maneuver provides direction for the development of artillery tactics in recent years , which reflects both the requirements for artillery systems and the ability to Fire for Effect.

Keywords— artillery, artillery battle formation,* firing data and firing method, *conflict between Russia and Ukraine.

I.INTRODUCTION

The role of artillery is its participation in the fire-strike of the targets and objects of the opposing forces on the battlefield, with the conflict in Ukraine being its most significant use in the modern era in terms of rifled and rocket artillery [1].

In the armed conflicts of recent years between conventional armies, artillery has been a key tool for adapting to counter enemy tactics and is a major factor in slowing or stopping offensive actions [2]. This statement follows from the analyses of the war in Ukraine [3] and the conflict in Nagorno-Karabakh between Armenia and Azerbaijan [4]. However, artillery alone cannot propel any side to victory [5], but together with other areas of military affairs, its importance to the innovations and technological developments that found their way into the Ukrainian conflict of 2022 [6] is significant.

In this context, the limited use of aviation by the Armed Forces of Ukraine (AFU) and the Russian Federation (RF) in the armed conflict in Ukraine from 2022 to the present day is a litmus test that has led to an increased role for artillery [7], [8].

Various analyses indicate that The king of battle [9] has caused the most casualties on both sides, reaching 70-80% from indirect fire, artillery, multiple launch rocket systems, and mortars [10] - [11].

Artillery has acquired a new look with the changing dynamics of the battlefield, especially with the use of electronic warfare, which has further increased its share in combat operations. This is due to combat performance, which shows the advantage as a means of fire destruction in modern conflicts. artilleri units has the ability to fire in all weather conditions, regardless of the time of day or night, and to perform fire missions over wide areas and at great depths. Use different various technologies for detecting targets, correcting fire, assessing damage, and increasing the effectiveness of the use of unguided munitions, it has led to a logical change in its use.

In the paper, the author analyzes the change in the order of battle of artillery formations, imposed by modern battlefield dynamics, in combination with innovative intelligence tools, and emphasizes the change in the use of methods for determining firing data on both sides of the Ukrainian conflict.

II. MATERIALS AND METHODS

The use of literary sources and the data indicated in them from direct participants in the conflict between Russia and Ukraine, related to the combat use of artillery, is the basis for an analysis of the imposed changes in the

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8464
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

practical application of the issue under consideration, combined with other statements. The data traces the object of the study by dividing the changes in the order of battle and determining the data for firing to hit targets and objects, influenced by the specifics of the conflict and the transformation of artillery in the analyzed directions.

Various scientific methods have been used to analyze the transformation of artillery in the conflict – scientific analysis and synthesis, argumentative analysis, analysis of individual statements. The temporal change from the beginning of the conflict to the practical applications of the indicated data has been traced.

III. RESULTS AND DISCUSSION

A. Battle formation

The Armed Forces of Ukraine are changing the tactics of using artillery formations at the front [12]. The choice of firing positions based on the experience of the war has shown that it has undergone a transformation in relation to tactical standards [8] regarding the line of contact of the warring parties.

One of the reasons is the introduction of various artillery systems with greater range, and on the other hand, protection from enemy counterattacks. It is characteristic to carry out fire missions from firing positions, allowing to defeat the enemy and quickly change the battle order of the firing units in areas beyond the reach of the enemy artillery.

When saturating the battlespace with more places for firing positions, artillery reconnaissance groups play a primary role in their selection and preparation [8].

The destruction of targets (objects) by artillery formations is carried out by the warring parties with one maximum of two guns [8], thanks to the greater range and equipment with ground-based or satellite navigation systems and computerized automated fire control systems, which are capable of reducing activities to fire from a single gun (combat vehicle) [13].

Other factors influencing this choice are protection from enemy fire and the need to reduce the time spent at the firing positions, which are skillfully compiled with the natural shelters of the area in combination with engineering facilities and compliance with radio discipline (emissions control - EMCON) with limited use of mobile phones.

These so-called facilities are in most cases created with improvised materials, having a wood-earth character, but necessarily covered with a net to counter unmanned aerial vehicles.

Colonel Baranov was selected by the Chief of Defence staff to prosecute the Artillery war, specifies that there should not be one common area for all guns in one formation, but it is necessary for the battery command post to be in a protected place between the firing positions, preferably in a dugout (or on a mobile base), calling the battle formation a dispersed battery [14].

This tactic is also confirmed by Serhii Musiienko, deputy commander of the Ukrainian Armed Forces Rocket and Artillery Forces, pointing out that the platoon commander, a senior officer of the battery, no longer controls all the guns of the battery or platoon at the location of the firing position, and the artillery is dispersed, because such an arrangement leads to the disclosure of the positions and is threatened by enemy counterattack [12].

The characteristic of this battle formation is the firing positions of individual guns, characterized by autonomy for the execution of fire tasks from one means of destruction, directly communicating with another gun from a distance. The ability to fulfill the task of dispersing fire positions is through the use of automated fire control systems (AFCS) and the availability of means for determining the coordinates of each gun, and the data transfer is through various communication channels. The AFCS calculates individual data for each gun that has received a fire destruction task, determining the corrections for the data for hitting targets from the same or other guns in the unified fire control system for a division, battery or platoon for a specific area for the execution of the assigned tasks.

To perform a fire mission, the gun (or guns) receive the data from the AFCS for firing, take up firing positions, perform the task in a short time frame and leave the position, taking up the next one or taking cover. During this time, the battery command post does not change its covert location. Data transmission can be carried out in several ways:

- From the battery command post to the guns of the artillery formation;
- From one gun to the others (in some countries that have provided artillery systems to Ukraine, the platoon commander is located in one of the guns of the platoon, therefore there is no separate battery command post;
- The guns receive a list of target data that they can call from the AFCS individually without the intervention of communication channels, so as not to reveal the lines of communication and compliance with radio discipline.

Determining the coordinates of each gun's locations can be determined by:

- GPS receiver in the gun, connected to the AFCS;
- GPS receiver of the radio station in the gun;
- Other methods (geodetic tasks) in case of impossibility of using GPS, which always require more time, but still cannot be ruled out.

This battle formation, indicated by the Ukrainians, was applied after analyzing the experience of the combat operations of the opposing side in the conflict, using artillery in a classic battle formation, linear deployment with a distance between the systems of 20-50 m. and 200-300 m from them of the vehicles for transporting ammunition. When hitting these trucks, which are 5-6 in number, piled up in one place with shells, it led to chaos in

the firing position and to the incapability of the entire formation (battery or platoon).

To fulfill their tasks, Ukrainian artillerymen prepare up to 8-9 firing positions for one battery (platoon) in one area for combat use, and also replace the firing positions from towed artillery, which analysts [13] define as an innovation.

To protect against counterfire, the Russians in certain cases do not change the positions of the guns, and the crews hide in previously prepared places, and in other cases they also switch to a dispersed arrangement [15] of the firing position.

Analyzing the actions of the Russian artillery formations, it can be stated that they (according to data from an interview with a commander of a 152 mm self-propelled howitzer Msta-S, participating in the operation) first take up a firing position, prepare the gun for firing, carry out the firing task and leave the firing position, returning to their permanent cover, which is repeated about 5-6 times within one combat day [15]. The Russian artillerymen define the above actions as an artillery carousel, the analysis of which was carried out by the author in the report "Is the method for use self propelled and multiple rocket launcher systems new – artillery carousel" [16].

Other data indicate that the order of execution of a fire mission is reduced to determining the firing data of the gun(s), their transmission, taking up a firing position, firing to defeat, in a time range of 2-3 minutes for the guns or volley fire from combat vehicles from MLRS for up to 20 seconds [8], leaving the firing position, calculating data for the next firing mission and taking up the next firing position or concealing the firing guns in relation to the terrain and their mobility.

The differences in the two methods can be distinguished in several key points. The first of these is receiving the firing mission. From a theoretical point of view, this should be done before any movement of the gun is made in order not to violate its camouflage and after readiness, with known data on hitting the target, to take up the firing position and open fire, as indicated by the data of Orkushpaev and his colleagues in the report "Combat work of artillery fire units in modern armed conflicts" [8]. On the other hand, there is the practical application, in which receiving the task after taking up and preparing the firing position will unmask the actions of the calculation earlier and expose them with a greater probability of counteraction from the opposing side, which points to the second key point – the time of stay in the firing position. Taking up a firing position without a fire mission assigned can be defined as an error in the command and control system, because taking up a prepared firing position and preparing it for fire will increase the total gun dwell time by at least one minute.

The third pillar of the analysis is the artillery system commander's statement that "we are returning to our permanent location" [15]. It is easiest to point out problem areas when someone else is performing the tasks, but constantly occupying the same hiding place also leads to the disclosure of the locations of not only one, but also several artillery systems, as a result of the adopted method of maneuvering in the firing position area, although indicated by an assessment of the situation or imposed by various factors. In this context, if something can be observed and defined as a target on the battlefield, the impact from the opposing side is almost possible in a short time interval, evident in the Second Nagorno-Karabakh War in 2020, but with a huge emphasis for the war in Ukraine from 2022, because indications show that the Ukrainians are destroying Russian guns at a significantly increased rate. If this data is correct, this could mark a turning point in the war. This may also be a sign that traditional artillery is vulnerable, not only to new types of weapons [1], but also to traditional ones [2] when accumulating various beams, affecting factors - time for the execution of fire tasks and unmasking one's own positions.

B. Determination of firing data and firing method

In the initial phase of the Ukrainian conflict, the determination of firing data and firing method was carried out uniformly by different methods [19], [20], a statement from an analysis based on the theoretical documents of both sides of the conflict. The presence of artillery fire shows the historical commitment to the Warsaw Pact and the available unified system in its member states. The author of this report is not a supporter of the methods for determining firing data through them, because their implementation does not correspond to the dynamics of modern combat and the reasons are:

- Unmasking the positions of the gun, performing the task of firing at a target or creating benchmarks;
- Significantly increasing the stay at the firing position by over 7-10 minutes;
- Using reconnaissance forces and means that can be detected by the opposing side with subsequent impact (laser rangefinder);
- Blocking a fire resource (gun) to perform this task;
- Need for additional quantities of ammunition.

It is true that using data from various methods of adjustment (of fire) from one target is the most accurate way to determine the days for firing at other targets in artillery, but analyzing its shortcomings, it is preferable to initially use AFCS with calculation through full preparation, and subsequently use data from fire strikes from other targets with the same or other firepower, as indicated by the authors in the report "Combat work of artillery fire divisions in modern armed conflicts" [8]. The same analysis for both the Second Nagorno-Karabakh War in 2020 and the armed conflict in Ukraine in 2022 is also made by Leonid Nersisyan, indicating that traditional approaches to artillery fire control are not particularly effective on the modern battlefield compared to digital solutions [21]. Research shows that without a certain level

of digitalization, too much reliance is placed on the mass of fire to achieve the necessary effect. Legacy systems used in large batteries become much easier targets in counter-battery combat, especially when staying in firing positions for a long time.

In this line of thought, by adopting software-defined warfare, Ukraine has gained an advantage in two areas where Russia was thought to have a decisive superiority: artillery and cyberwarfare [22]. By using software applications, Ukraine's artillery has carried out significant fire missions with great accuracy against Russian forces, despite the superiority of the opposing troops. This was also achieved through the use of modern means of reconnaissance and target data acquisition (various types of drones, counter-battery radar systems (1L221E), etc.), as well as the skillful application of the same in counter-battery combat. Ukraine has also successfully dealt with Russian cyber threats, thanks to the IT sector, which has received a favorable development environment, leading to development and innovation.

IV.CONCLUSIONS

Artillery has undergone many transformations from its initial adaptation in 618 BC, according to ancient Chinese chronicles, to the present day artillery. Changes marked by victims from various conflicts have left their mark on the methods of its use.

The concepts of the order of battle of artillery formations established since the end of World War II were long established as postulates, but the dynamics of the development of the modern digital battlefield led to a perhaps expected breakthrough in breaking the icy traditions of this arrangement.

The use of the cannon alone, at least for the post-Soviet military school, was for performing tasks to mislead the enemy, but with ambiguity in the operational picture of the battlefield, but the armed conflicts after 2020, to a greater extent between Russia and Ukraine, led to the transformation analyzed in the report, written with the blood of hundreds of thousands of victims from the opposing sides. The battle formation in various geometric shapes was washed away like a sand figure by the waves of the ocean, to give way to the power of using one or two firepower to defeat the enemy with the full support of digitalization and automation of the processes of detecting artillery fire on a target or object.

The changes imposed in the artillery order of battle are a consequence of the new concepts of hitting targets with reduced ammunition consumption at the expense of increased accuracy. The application of the method of firing with one or two guns is successfully combined with the use of covert maneuver and an increased number of free fire resources (from the rest of the artillery formation) for performing other tasks in the fire support system, as well as reducing the vulnerability of the formation in counter-battery combat.

The stealth, surprise and accuracy of artillery are now a priority for those using it, with the element of surprise coming not from the "beautiful" target exchanges, as the traditionalists called them, but from the use of AFCS data, which apply in real time corrections for the various factors affecting the accuracy of artillery fire.

The advent of various means of determining the location of targets has had a beneficial effect on the large number of observable targets, drastically changing the concepts of planning fire strikes on both sides of the conflict. This in turn has an impact on the procedures for determining the method for determining firing data, due to the provision of real-time data on the state of damage and the resulting effect.

REFERENCES

[1] D. Saw, "Balancing the Artillery Picture," European Security & Defence, October 25, 2023.

[2] L. A. Oltei, J. Potin and E. Clarke, F I N A B E L - European Army Interoperability Centre, January 2024.

[3] J. Bosbotinis, "The Lessons of the Ukraine War and Its Implications for Artillery," Institute for Defense and Government Advancement, 2023

[4] G. Gressel, "Military lessons from Nagorno-Karabakh: Reason for Europe to worry," The European Council on Foreign Relations, November 24, 2020.

[5] I. Daalder, "Stalemate best describes the state of war in Ukraine," Politico, November 27, 2023.

[6] B. Ivanov, "Razvitie na bezpilotnite nadvodni i podvodni aparati vav voynata na Rusia sreshtu Ukrayna," Sigurnost i otbrana, no. 1, pp. 310-321, June 2024. [Б. Иванов, "Развитие на безпилотните надводни и подводни апарати във войната на Русия срещу Украйна," Сигурност и отбрана, no. 1, pp. 310-321, Юни 2024].

[7] A. Fedotov and E. Pudovkin, "«Bog voynы». Pochemu artilleria stala glavnым faktorom v boevыh deystviyah na Ukraine i chto эto znachit dlya hoda srazheniy," Apr 29, 2023. [А. Федотов and Е. Пудовкин, "«Бог войны». Почему артиллерия стала главным фактором в боевых действиях на Украине и что это значит для хода сражений," 29 04 2023]. [Online]. Available: https://rtvi.com/stories/bog-vojny-pochemu-artilleriya-stala-glavnym-faktorom-v-boevyh-dejstviyah-na-ukraine-i-chto-eto-znachit-dlya-hoda-srazhenij/ [Accessed July 16,2024]

[8] E. M. Orkushpaev, R. Zh. Ibragimov, R. M. Zhambirov and D. M. Abdыbekov, "Boevaya rabota ognevыh podrazdeleniy artillerii v sovremennыh vooruzhёnnыh konfliktah," ҚӘӘІ HABARShЫSЫ, July 2024. [Е. М. Оркушпаев, Р. Ж. Ибрагимов, Р. М. Жамбиров and Д. М. Абдыбеков, "Боевая работа огневых подразделений артиллерии в современных вооружённых конфликтах," ҚӘӘИ ХАБАРШЫСЫ, 07 2024].

[9] V. Mittal, "Artillery Is Still The King Of Battle In The Russia-Ukraine War," Forbes, July 17, 2024. Available:.https://www.forbes.com/sites/vikrammittal/2024/07/16/artillery-is-still-the-king-of-battle-in-the-russia-ukraine-war/ [Accessed Dec. 20,2024]

[10] D. Rice, "Cluster Munitions Have Changed the Course of the Ukraine War," Small War Journal, December 29, 2023.

[11] P. Turchin, "Empirically TesӨng PredicӨons of an AΣriӨon Warfare Model for the," Cliodynamic Technologies LLC, November 2023.

[12] S. Biddle, "Back in the Trenches: Why New Technology Hasn't Revolutionized Warfare in Ukraine.," Foreign Aff, 2023.

[13] L. Oleniak, "Ukraine changes tactics of using artillery: Peculiarities," RBC - Ukraine, November 18, 2024.

[14] N. Świętochowski, "Field Artillery in the defensive war of Ukraine. Part I. Combat potential, tasks and tactics," Scientific Journal of the Military University of Land Forces, vol. 55, pp. 341-358, 2023.

[15] S. Baranov, "Using artillery in complex environments lessons from the Ukrainian front," in Future Artillery Conference, 2023.]. [Online]. Available: https://eco-cdn.iqpc.com/eco/files/event_content/futart-ukraine-complex-environmentstdfinal-of-finalH1FkB0flPC3dB9cUwOvvprv9Tp8myvm12mkeWMGI.pdf [Accessed Dec. 10,2024].

[16] A. Sharkovskiy, "Rossiyskie samohodchiki primenyayut taktiku - «artilleriyskaya karusely»," Argumenty Nedeli, December 23, 2023. [А. Шарковский, "Российские самоходчики применяют тактику - «артиллерийская карусель»," Аргументы Недели, 23 12 2023].

[17] D. Markov, "Nov li e sposobat za boyno izpolzvane na samohodnata i reaktivnata artileria – artileriyska vartelezhka," Godishna universitetska nauchna konferentsia, 2019. [Д. Марков, "Нов ли е способът за бойно използване на самоходната и реактивната артилерия – артилерийска вртележка," Годишна университетска научна конференция, 2019].

[18] D. Hambling, "How Is Ukraine Destroying So Much Russian Artillery?," Forbes, July 17, 2024.

[19] M. Stefanov, Boyni deystvia vav visokoplaninska sreda, Veliko Tarnovo: Nats. voen. univ. "Vasil Levski", 2021. [М. Стефанов, Бойни действия във високопланинска среда, Велико Търново: Нац. воен. унив. "Васил Левски", 2021].

[20] S. A. Bakaneev , S. A. Orlov and Yu. M. Chernышev, Prakticheskiy kurs. Bloknot po strelybe i Upravleniyu ognem., Sankt–Peterburg, 2023. [С. А. Баканеев , С. А. Орлов and Ю. М. Чернышев, Практический курс. блокнот по стрельбе и управлению огнем., Санкт–Петербург, 2023].

[21] Gorbilyov at al, Pravila strilybi i upravlinnya vognem nazemnoї artilerії (divizion, batareya, vzvod, garmata), Kiïv: Ministerstvo Oboroni Ukraïni, 2017. [Горбильов at al, Правила стрільби і управління вогнем наземної артилерії (дивізіон, батарея, взвод, гармата), Київ: Міністерство оборони україни, 2017].

[22] L. Nersisyan, "Modern artillery fire control equipment is a requirement for all armed forces," European Security Defence, March 05, 2024.

[23] D. Zikusoka, "How Ukraine's "Uber for Artillery" is Leading the Software War Against Russia," May 23, 2023.

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 185-189

Influence of Armed Conflicts on Methods for Determining Firing Data for Hitting Artillery Targets

Dilyan Markov
Rakovski National Defence College
Sofia, Bulgaria
dilyanmarkov@abv.bg

Abstract* — *In recent years, fire automation has entered the artillery area with full force, which together with the introduction of visualization from various sources on the battlefield, has led to changes in the methods for determining the data for firing at the targets of the opposing forces. Real combat operations have become a springboard for practical testing of various procedures in this direction. The presence of an enemy seeking to counter artillery fire additionally, through active actions, has reduced the time for performing fire tasks and imposed the need for changes in the determination of fire data for hitting targets of different nature. Historically, this is another step towards improving the effectiveness of fire and maneuver of artillery fire support means, especially for older models, which are still used in the space saturated with artillery systems of modern conflicts.

Keywords* — *artillery, data on the target, fire control procedures fire support

I.INTRODUCTION

Historical information indicates that artillery firing methods are based on in-depth theoretical research, data from experimental range exercises conducted in the pre-war years, as well as a summary of experience from the combat use of artillery.

In the context of the above, the actions of the Russian artillery, which entered the Second World War with the 1939 rules of fire (ПС-39), were defined as quite modern and sufficiently scientifically sound. All artillery firing methods introduced at that time were based on adjustment methods after firing from a cannon taking up 10–15% of the total time allocated for artillery preparation [1].

However, the fighting in 1941–1942 showed that the provisions and recommendations of these shooting rules did not always correspond to the specific combat situation [2] and in 1942 new Shooting Rules (ПС-42) were published, which remained the main guide until the end of the war.

In this line of analysis of data from a number of local and global conflicts in recent years using artillery formations, the methods for preparing the initial data for firing at the targets of the opposing forces are an element of combat use that undergoes changes on the battlefield together with changes in tactical actions.

With the introduction of various means of observation on the battlefield, artillery targets become observable and data on them can be determined with sufficient accuracy for the needs of fire destruction. The use of modern automated means of fire control of artillery formations, on the other hand, provides the necessary litmus for changes in artillery firing procedures in the direction of increasing the effectiveness of destroying opposing forces.

In this direction, the results of the battlefield provide the approved beams for the development of various procedures applied to achieve the necessary effects.

II. MATERIALS AND METHODS

The use of literary sources and data from the combat use of artillery is the basis for analyzing the indicated changes in the practical application of the issue under consideration, combined with the need for changes in the procedures for this based on practical experience and logical-investigative connection.

The indicated data compare the object of study over the time horizon for the need for changes in the procedures and determination of the shooting data for hitting targets and objects, influenced by the specifics of modern conflicts and the transformation of artillery.

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8477
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

Various methods were used to analyze the combat use of artillery - scientific analysis and synthesis, argumentative analysis, analysis of individual statements.

III. RESULTS AND DISCUSSION

The effectiveness of fire is achieved by obtaining reliable and accurate data on the location, size and nature of targets, the correct choice of means of hitting the target, high accuracy and suddenness of fire, the appointment of an appropriate order for the execution of the fire task and methods of firing at targets.

The accuracy of fire depends on the determination of the firing data bytargets and is achieved by using the most accurate methods for this, as well as by correcting the fire in the course of firing for hitting. It is one of the factors influencing the effectiveness of fire.

According to the theory of artillery shooting, the main method for determining firing data is considered to be complete preparation - Accurate Predicted Fire (APF), due to the fact that the data obtained on its basis allow hitting targets without observation, but ensuring the speed and suddenness of opening fire. With the advent of a number of means of observing targets, the shooting rules used have significantly expanded the scope of application of the most accurate method for determining firing data - by using an adjustment gun.

It is through the use of surveillance, such as the introduction of unmanned aerial vehicles into the artillery, as one of the main types of artillery reconnaissance that the majority of targets that are hit even at maximum firing distances pass into the category of observed targets [3]. This leads to a reduction in collateral losses and a significant reduction in ammunition consumption.

The available data on ammunition consumption for hitting unobservable targets specified in the firing and fire control procedures are calculated based on the indicators of complete preparation, correlated with the methods of firing at different types of targets. However, in a combat situation, the implementation of all the activities envisaged to achieve the conditions of complete preparation is difficult due to the limited time [4].

Technical support for conducting meteorological and ballistic preparation activities for firing, which have the greatest impact on the accuracy of complete preparation, is difficult to achieve in a limited time frame. The main drawback of existing methods for performing fire tasks is the presence of procedures without taking into account the capabilities of automated fire control systems and reconnaissance systems. Therefore, the improvement of methods for performing fire tasks implies the further development of methods for determining firing data, selecting the type of projectile, the installation of the fuse, methods of firing at individual and group targets and the order of performing fire tasks, as well as parameters that determine decision-making and the execution of a fire task, taking into account modern and promising automated fire control systems and fire correction complexes [3].

The modern battlefield is saturated with a wide variety of targets requiring the use of not only high-explosive fragmentation shells, but also special-purpose ammunition - thermobaric, volumetric detonating, remote mine and incendiary, and to improve efficiency, it is necessary to apply, created on new physical principles, as well as non-lethal ones, such as shells with a contusion-traumatic effect to defeat open and hidden manpower, with microwave generators to affect communication equipment, optoelectronic devices and electronic control equipment, as well as against internal combustion engine shutdown units and electrically conductive elements to shut down power lines, substations and control elements of electrical units [3] and, therefore, develop or correct appropriate procedures for their use.

Such procedures, which will improve the methods of performing fire tasks, by developing methods for determining the firing data, the choice and type of projectile and the installation of the fuse.

Analysis of currently active armed conflicts indicates time as an important factor, showing that artillery formations must open fire to hit enemy targets after taking up a battle formation, without delay. In accordance with the requirements, this time takes up to 3 minutes [5] [6], as the gun crew has time to deploy, perform the fire task and leave the firing position or between 3 and 5 minutes after detecting a target [7], in order to minimize the risk of a retaliatory strike.

These times for modern artillery systems are easily achievable, due to the automation of the guns themselves and the availability of automated fire control systems (AFCS), compatible with various systems for providing target data and communication and information support systems. Many artillery installations are used on the battlefield in various armed conflicts, without the specified systems and achieving the task execution times is a challenge, especially in the highly dynamic operational environment. For this reason, to facilitate the activities of determining the data for firing at artillery targets, a number of applications are used, based on smartphones or tablets, leading to increased speed in mathematical problem solving and minimizing the human factor of making errors, leading to failure to complete the assigned tasks.

In this direction, a digital ecosystem is being mobilized in Ukraine, a component of a developing “geometry of force”[12], oriented towards the purposes of a country’s defense. A number of applications have been created and used in this area, such as УКРОП, КРАПИВА, ГИС АРТА, etc.

Looking at the focus of the problem, it can be stated that the Second Nagorno-Karabakh War in 2020 and the armed conflict in Ukraine since 2022 show that the traditional approaches used in artillery firing procedures,

the determination of firing data and the control of artillery fire are not particularly effective on the modern battlefield. For this purpose, the indicated solutions in digitalization, through applications, have been used.

The difficulties without digitalization represent a difficult gap for artillery to overcome. The main reasons lie in the following areas:

- the presence of technical means for determining firing data, which limit the spatially used artillery systems (different fire control means);
- the use of different tables for determining firing data, in which the values are manually interpolated;
- the presence of paper topographic maps of areas, which are inaccurate in terms of changes and infrastructure and areas over the years;
- differences between angular sizes - from 64-00 mils for NATO and 60-00 mils for post-Soviet artillery systems.
- The determination of firing data to hit enemy targets by using the most accurate method for this, by using an adjustment gun, is distinguished by certain characteristics that do not correspond to the modern dynamics of the battlefield:
- use of a gun system only for this activity, which takes away from the fire resource of the artillery support system;
- increased ammunition consumption;
- increased time spent at a firing position of a firing gun;
- unmasking of the position of the firing guns.

A characteristic feature of the determination of the data for firing for hitting under the concepts of work without automated fire control systems is the manual work in determining the corrections due to the change in the conditions of meteorological and ballistic preparation and taking into account the technical preparation for each artillery system. This activity is laborious and requires personnel for each preparation in combination of activities between them. The time for modern dynamic combat is enormous for this activity, including calculations with the possibility of numerous errors made by the calculators. From another point of view, the interpolation of the values from the tables for data for the relevant preparations leads to an increase in the values of the discrepancies with the real values.

For this and other reasons indicated in the presentation on the topic, changes in the determination of the data for firing for hitting targets are necessary, which correspond to the realities.

The changes resulting from this, according to the author, need to cover certain areas.

The first of them is related to a rather case-related question of how the data on the first target will be determined? In reality, on the battlefield, before opening fire from a certain artillery piece, there is no data on previously conducted actions to fire a target. For this reason, the data would be determined by the method of complete preparation when calculating the days of fire control systems when compared with tabular data on changes in firing conditions. This activity is carried out by various AFCS currently in service.

In the absence of AFSC, computer applications similar to those specified in Ukraine can be used with sufficient accuracy to perform the task at hand, because Ukraine has learned to “transform a simple piece of metal from the Cold War era into a combat unit integrated into a digital combat system that allows for a completely new way of fighting” [8]. Here lies the problem. Taking into account the changes, these applications successfully perform the tasks for which they are intended, and until years ago it was impossible to implement them as unapproved software in the fire support system.

Such a problem is the admission of such software on different platforms. An example is the blocking of УКРОП by Apple due to violation of paragraph 1.4.5 of the rules [9], because such software is used in combat zones and can cause harm to people.

Subsequently, the development of such mobile applications, through the more active use of awareness systems, voluntary and private initiatives related to artificial intelligence, as well as crowdsourcing of data, the use of open source platforms and progress in the decentralized use of relevant assets in Ukraine, has acquired a new dimension. Since 2023, the Cabinet of Ministers has begun to more systematically launch policy initiatives for the advancement of artificial intelligence in the field of defense, for the advancement of the relevant national industrial base, the creation of a new ecosystem and progress in public and private financing solutions [10].

Russia is also waging network warfare, using a computerized command and control system to consolidate the operations of drones and artillery batteries [8].

Thus, the armed forces adopt such software applications, which allows them to be implemented in various procedures for determining firing data for hitting targets.

The second area is the use of firing data for hitting artillery targets for subsequent ones.

Many analysts would point out that this is a routine activity and is already being carried out. This is so according to current procedures, but for conventional ammunition and targets, the nature of which is specified in the current rules. The report indicated the transformation of targets and the use of new types of ammunition, as well as the calculation of ammunition consumption, because

computer determination of firing and guidance data saves about 15-30% of shells [8]. With these changes, an update of the entire procedure for determining the method of firing at targets is necessary, as a result of these changes. An important part is also the increase in the accuracy of artillery fire, by applying various techniques. This in turn reduces the ammunition used. In fact, one activity in this direction - determining the firing data for hitting and the method of firing would be almost impossible without the use of fire control systems or software applications, with updated data on the systems, ammunition, target standards and open input capabilities for receiving shot data on targets

With these changes, an update of the overall procedure for determining the method of firing at targets is necessary, as a result of these changes. An important part is also the increase in the accuracy of artillery fire, by applying various techniques. This in turn reduces the ammunition used. In fact, one activity in this direction - determining the data for firing for destruction and the method of firing would be almost impossible without the use of fire control systems or software applications, with updated data on the systems, ammunition, target standards and open access capabilities for receiving target firing data. In this direction, the inclusion of artificial intelligence would be a good implementation towards improving the capabilities of fire support assets, taking into account and applying static and dynamically changing battle formations, measures for coordinating fire support, joint targeting, etc.

AFCS are not a panacea for solving these problems. In reality, the application of certain procedures for artillery firing has its limitations, which serve as postulates in the theory of firing.

The theory of artillery firing sets limits for the transfer of fire in a range of no more than 3-00 in direction and 4 km in distance from the firing of fire at a fictitious or real target. To increase the range of artillery systems, this spatial limit is small, but in turn, in the area for the execution of artillery fire tasks, there is a certain amount of formations that fire at enemy targets. The accumulation of zones for the use of data on fire defeat would cover a significant perimeter of the location of the targets. Thus, the density of possible calculated data in the required accuracy would increase, but in order to use them fully, their constant reporting is necessary, not only for the specified spatial boundaries, but also in time, with a limitation of up to 3 hours from the conducted artiilery fire . This database would be a laborious task in the dynamics of the data flow, for which the sought-after solution remains automation. The contact point wth this is also important with the methods for determining the shooting data, because restrictions are also imposed on the specified heights of the trajectories to achieve the required hitting effect, which in mortar fire significantly reduce the spatial boundaries to 1 km.

All this leads to the desired result of increasing the effectiveness of artillery fire in conjunction with improving the methods of operation of the control bodies when performing fire tasks, because it is precisely in these cases that, if there is insufficiently effective control, 25-35% of the artillery's capabilities can be lost [3].

IV.CONCLUSIONS

The use of new models of weapons and ammunition, as well as increased range, rate of fire and the use of control systems, as well as the requirements for updating the procedures for firing and fire control, are the paths of development of modern artillery.

The need for stealth, surprise and accuracy, as principles for the use of artillery, leads to the use of means that differ from the technical means used over the years. To this end, it is necessary to replace them with software applications adaptable to the overall digitalization of the battlefield, which will lead to an increase in capabilities, as a force multiplier and will give an advantage over enemy forces.

The digitalization of artillery cannot be an obstacle to its development, as was claimed in the past, when even the training of artillery specialists using electronic calculators was prohibited. The digitalization of military technologies reflects the opposition between old and new ways of waging war [8]. It is present in software-based warfare and must be accepted as a mandatory step in its development. On its basis, it is necessary to update the postulates in artillery with regard to the analyzed problem related to the determination of data for firing at artillery targets.nation of data for firing at artillery targets.

V. ACKNOWLEDGMENTS

This work was supported by the NSP SD program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022

REFERENCES

[1] M. Kirillov-Gubetskiy, Sovremennaya artilleria, Moskva, 1937. [И. М. Кириллов-Губецкий, Современная артиллерия, Москва, 1937].

[2] G. E. Peredelyskiy, A. I. Tokmakov and G. T. Horoshilov, Artilleria v boyu i operatsii, Voenizdat, 1980. [Г. Е. Передельский, А. И. Токмаков and Г. Т. Хорошилов, Артиллерия в бою и операции, Воениздат, 1980].

[3] A. G. Musin, "Povышenie эffektivnosti podgotovki i upravlenia raketnыmi udarami i ognem artillerii: problema i puti reshenia," in AKTUALYNЬIE PROBLEMЫ ZAShtITЫ I BEZOPASNOSTI, Sankt-Peterburg, 2019. [А. Г. Мусин, "Повышение эффективности подготовки и управления ракетными ударами и огнем артиллерии: проблема и пути решения," in АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ И БЕЗОПАСНОСТИ, Санкт-Петербург].

[4] V. V. Kozlov and M. Yu. Muhin, "Povышenie эffektivnosti ognya artillerii primeneniem metoda passivnoy pelengatsii snaryada v hode pristrelki tseli," VOENNAYa MЫSLY, vol. 7, 2022. [В. В. Козлов, М. Ю. Мухин, "Повышение

эффективности огня артиллерии применением метода пассивной пеленгации снаряда в ходе пристрелки цели," ВОЕННАЯ МЫСЛЬ, vol. 7, 2022].

[5] D. D. Babaev, "Osobennosti sredstv podgotovki strelyby i upravlenia ognem perspektivnыh artilleriyskih kompleksov.," Mirovaya nauka, vol. 8, no. 41, 2020. [Д. Д. Бабаев, "Особенности средств подготовки стрельбы и управления огнем перспективных артиллерийских комплексов.," Мировая наука, vol. 8, no. 41, 2020].

[6] E. M. Orkushpaev, R. Zh. Ibragimov, R. M. Zhambirov and D. M. Abdыbekov, "Boevaya rabota ognevыh podrazdeleniy artillerii v sovremennыh vooruzhënnыh konfliktah," ҚӘӘІ HABARShЫSЫ, Jul 2024. [Е. М. Оркушпаев, Р. Ж. Ибрагимов, Р. М. Жамбиров и Д. М. Абдыбеков, "Боевая работа огневых подразделений артиллерии в современных вооружённых конфликтах," ҚӘӘИ ХАБАРШЫСЫ, 07 2024].

[7] N. Święchowski, "Field Artillery in the defensive war of Ukraine. Part I. Combat potential, tasks and tactics," Scientific Journal of the Military University of Land Forces, vol. 55, pp. 341-358, 2023.

[8] D. Shashank, "Uber dlya artillerii. Kak novыe i staryе tehnologii smeshivayutsya i sorevnuyutsya na voyne v Ukraine," Mediazona, Jul. 23, 2023. [Д. Шашанк, "Uber для артиллерии. Как новые и старые технологии смешиваются и соревнуются на войне в Украине," Медиазона].

[9] "Apple zablokuvala programne zabezpechennya UKROP," 2019.["Apple заблокувала програмне забезпечення УКРОП," 2019. [Online]. Available: https://www.ukrmilitary.com/2019/05/apple-against-ukrop.html [Accessed Feb. 06, 2025].

[10] V. Goncharuk, The Very Long Game, Springer, Cham, 2024.

[11] S. A. Korolev, D. G. Nefedov and I. G. Rusyak, "Intellektualynaya sistema avtonomnogo navedenia i korrektirovki strelybы," Informatika, vыchislitelynaya tehnika i upravlenie, vol. 22, no. 3, p. 85–91, 2024. [С. А. Королев, Д. Г. Нефедов and И. Г. Русяк, "Интеллектуальная система автономного наведения и корректировки стрельбы," Информатика, вычислительная техника и управление, vol. 22, no. 3, p. 85–91, 2024].

[12] M. Ford, "From innovation to participation: connectivity and the conduct of contemporary warfare," International Affairs, 2024

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 191-199

Tracing Reflexive Control Application in the Anti-Shale Gas Movements in Eastern Europe

Boyan Mitrakiev
dept. National and regional security
University of National and World Economy
Sofia, Bulgaria
bnmitrakiev@gmail.com

Noncho Dimitrov
dept. National and regional security
University of National and World Economy
Sofia, Bulgaria
bnmitrakiev@gmail.com

***Abstract*— Energy security and energy diversification have become key components of the European Union's response to the Russo-Ukraine war. While leveraging Green Deal instruments to boost renewable energy investment and replace coal and to some extent nuclear power generation, the Union has not been fully successful in its goals to secure energy independence from Russian energy supplies. The dependency on natural gas persists and has proven many of its critics wrong as the EU is currently importing gas from USA, Algeria, Norway and even Russia through various intermediaries. With domestic natural gas production decreasing, looking back to historic obstructions to developing new sources is justified from a national and regional security perspective. This article studies the anti-shale gas movements in the early and mid-2000s in Eastern Europe, which culminated in almost blanket bans on developing shale gas fields. Looking back at these events through the lens of a type of information warfare called reflexive control finds plausible evidence that such may have been applied in order for Russia to block or delay Eastern European efforts for energy security and energy diversification. Tracking the political behaviour and stances of the anti-shale movement leaders in the early and mid-2000s points to them holding a diverse array of opinions and contemporary positions concerning the Russo-Ukraine war and dealing with Russia in the area of energy today. This suggests that foreign information warfare and information interference could have targeted very basic elements and assumptions in the decision-making processes of civil society and state actors, which do not necessarily depend on their political perceptions of Russia. It is therefore possible to lay out and at least partially confirm a hypothesis that a reflexive control operation that substitutes and modifies such processes with new information concerning exaggerated and manipulated shale gas development risks might have been carried out by foreign state or non-state interested parties.**

Keywords*— *reflexive control, shale gas, energy, information warfare

I. Introduction

The 21st century has witnessed a significant evolution of information warfare as first the distribution and now creation of information have undergone processes of monumental transformation with the advent of social network services and artificial intelligence. However, theoretical concepts of information warfare strategy remain remarkably robust due to its dependency on human psychological characteristics such as the use of heuristics, biases, stereotypes, processing and perception of information, etc. One good example in lieu of this is the reflexive control type of information warfare – a Soviet-era concept which is now deeply embedded in Russian military and intelligence strategy. Reflexive control involves manipulating an adversary's decision-making process through carefully curated information, leading them to act in a manner advantageous to the manipulator. Even though Russian information warfare has developed throughout the last half a century, this theory has remained remarkably robust and effective, successfully integrating new information technology and information systems warfare without losing its central logos.

Taking into account the profound negative impact that restraining domestic natural gas production has had on European energy security and energy diversification during the Russo-Ukrainian war, it is thus prudent to hypothesize that external state or non-stake actors might have levied reflexive control principles in information warfare against the failed shale gas production in the early and mid-2010s.

Shale gas, heralded as a game-changer in energy politics due to its abundance and the technological breakthroughs in hydraulic fracturing or "fracking," posed both opportunities and challenges for Eastern European countries. Countries like Poland, Bulgaria, Romania, and others were seen as potential new frontiers for shale gas exploration, promising a reduction in dependence on Russian gas imports. However, these plans were met with

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8473
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

fierce resistance from local communities, environmental activists, and political groups, leading to widespread anti-fracking movements across the region.

The late 2000s and early 2010s were a time when the U.S. had demonstrated the viability of shale gas extraction, sparking global interest and investment in this resource. Eastern Europe, with its substantial potential shale reserves, became a focal point for energy companies looking to replicate this success, most notably the leader in shale gas development Chevron. However, the region's political, cultural, and environmental landscapes provided fertile ground for opposition and possible external intervention through information warfare.

II. Materials and Methods

A. Hypothesis

The hypothesis in this study is that state or non-state actors have implemented a reflexive control campaign against Bulgaria, Romania and Poland in the early 2010s when these countries attempted to explore and develop shale gas deposits.

In order for this hypothesis to be tested, the authors look into the ideological and political attitude of the leading anti-shale opinion makers in the four countries towards the Russian Federation and Russian energy supplies. Reflexive control campaigns by definition transmit information that is ingrained in the decision-making model of the adversary. On the basis of NATO's former chief Rasmussen's reasoning and declarations, the authors assume that state or non-state actors would have transmitted information that shale gas is environmentally harmful, which might have been integrated in the decision-making process of European opinion leaders of all political and ideological spectrums.

Therefore, the hypothesis would be partially confirmed if anti-shale opinion leaders are aligning in different and opposite camps regarding Russia's involvement in the Ukraine war and EU-Russia energy relationship rather than being organized in only one political camp. While the latter wouldn't automatically refute the hypothesis that a reflexive control campaign had been implemented, it would be much more likely that state or non-state actors had used other forms of information and intelligence methods, such as HUMINT.

B. Methods

The study is based on content analysis and more specific on textual analysis. Textual analysis in academic writing, particularly when analyzing news articles to understand the behavior of opinion leaders and politicians, is a methodical approach that involves several stages and techniques to dissect written content for deeper insight. When applied to news articles about opinion leaders and politicians, the goal is to understand not just what is said, but how it's said, why it might be said in that manner, and what the implications might be for public perception, policy, or political strategy. This analysis can reveal biases, framing techniques, rhetorical strategies, and the interplay between media and political power.

As a type of textual analysis, discourse analysis looks at language use in terms of the social context in which it is produced. Here, one would analyze how discourse around politicians or opinion leaders is constructed to serve particular political or ideological ends. In this study, discourse analysis will be targeted narrowly at the opinion leaders' and politicians' attitude towards the Russian federation's involvement in the Ukraine war and the Russian supplies of energy to the European countries.

C. Limitations

Reflexive control is an especially elusive information warfare to detect as it transmits only information that is intended to be (1) public and (2) fully perceived by the adversary. This means that analysts and the opponent can work only with assumptions and suggestions in hypothesizing, analysing, detecting and counteracting this information warfare tool.

Secondly, the anti-shale protests of the early 2010s were relatively massive and with a multitude of opinions leaders ranging from high-ranking politicians to grassroots campaigners who would later return to their non-public life and fade into information obscurity. Thus it is next to impossible to track the political alignment of all opinion leaders to present day on the topic of Russian energy and wartime policy.

Third, anti-shale activists that have not risen to international prominence may have continued to publish personal opinion in their own native languages (Romanian and Poland) which are difficult to search and find on social media and information databases.

Fourth, this article doesn't take any stance on the environmental integrity of any shale gas extraction methods or any hypothetical geological implications of the extraction itself. The authors recognize that different stakeholders may have different opinion on shale gas safety and the article's aim is not to address those but to discuss whether Russian state or non-state actors may have attempted to influence the decision-making process of EU states on this matter using a specific information warfare strategy.

D. Reflexive Control Theory

Reflexive control was conceptualized during the Cold War by Soviet military thinkers as a method to gain strategic advantage over the West. It aimed at controlling the adversary's thought processes, not just their actions, by feeding them information that would lead to predictable and favorable outcomes for the Soviet Union [1]. Over the decades, the tactics have evolved from traditional espionage to more sophisticated uses in information warfare, particularly with the advent of the internet and social media. Thomas [1] gives the following definition:

> …reflexive control occurs when the controlling organ conveys (to the objective sys-tem) motives and reasons that cause it to reach the desired decision, the nature of which is maintained in strict secrecy. The decision itself must be made inde-pendently. A "reflex" itself involves the specific process of imitating the enemy's reasoning

> or imitating the enemy's possible behavior and causes him to make a decision unfavorable to himself.

The essence of reflexive control lies in the manipulation of information, which is carefully curated and disseminated to shape how adversaries perceive their environment. This can involve a wide range of tactics, from spreading disinformation and misinformation to amplifying existing societal divisions or exploiting psychological vulnerabilities [2]. The goal is not simply to deceive but to create a distorted version of reality that leads the target to make decisions that serve Russia's interests as noted by Vasara [2]. For example, by flooding media channels with contradictory narratives or staging incidents that provoke specific reactions, Russia can create confusion and uncertainty, forcing opponents to question their own understanding of events. This manipulation is often subtle, designed to erode trust in institutions, sow discord, and destabilize societies from within and has become more refined and powerful with the advent of social networks and artificial intelligence. For instance, another scholar, Raskin [3] reviews the application of reflexive control in social networks specifically:

> Social networks have become an effective tool for managing public consciousness, directly influencing the decisions made by the leadership of countries in the context of escalating internal and international contradictions, conflicts, and crises. This facilitates the achievement of superiority in informational confrontations. […] When it is impossible to achieve a favorable balance of forces and weapons compared to the adversary, asymmetric actions become relevant. These include various methods of influencing decision-makers and public consciousness, one of which is reflexive management through social networks. Computer network technologies increase the effectiveness of reflexive management. Social networks create a virtual world filled with diverse information that circulates through direct communication between participants or through special actions organized by professionals. While users may believe they are accessing independent and objective information, moderators often control content flows, shaping users' perceptions and influencing their decisions

The effectiveness of reflexive control lies in its ability to exploit the inherent vulnerabilities of human cognition and modern information systems. People are naturally inclined to seek patterns and make sense of complex situations, and reflexive control takes advantage of this by presenting carefully crafted narratives that seem plausible but are ultimately misleading. In an era of information overload, where individuals and organizations are bombarded with data, the strategy thrives by adding noise to the signal, making it harder to discern truth from falsehood.

Countering reflexive control is a formidable challenge, as it requires not only detecting and debunking misinformation but also understanding the deeper strategic intent behind it. Traditional responses, such as fact-checking or public education campaigns, are important but often insufficient, as they address the symptoms rather than the root causes of the problem as discussed by Mitrakiev and Dimitrov [4], [5] and need to be supplemented by other methods for instance in the realm of democratic and social resilience as argued by Tagarev and Fluri [6].

III. Results and discussions

A. Poland

The US Department of Energy estimated in 2011 that Poland holds the largest potential reserves of shale gas in Europe [7]. A generally pro-US public attitude and a good regulatory framework allowed for Poland to make more shale gas exploratory drilling than any other European country as the governments have had expectations for any gas deposits to partially offset the closing of coal mines and power plants. Polish anti-shale movements have been active, however, with the Occupy Chevron series of protests being the most publicized. In June of 2013, members of this anti-fracking group occupied a field near the Polish village of Zurawlow, near the city of Zamosc.

Anti-shale campaigners in Poland had been mostly grassroots activists who haven't decided to maintain a high public profile after their successful protests against the natural gas development projects. There are a few exceptions of activists, mostly associated with international environmental NGOs, who have been active throughout the decade since the early 2010s such as Kuba Gogolewski and the ClientEarth leaders.

Kuba Gogolewski has been one of the most prominent anti-shale activists in Poland. The NGO activist has led several campaigns aimed at the government, oil companies, financial institutions [8] and others supporting shale development in the country. In 2013, Gogolewski [9] argued against the Polish government's moves to limit the influence of campaign groups who opposed fracking:

> If you really believe shale gas is the way forward and would be fully accepted by society you should actually strengthen the local regions and communities. Poland is a black horse on climate issues and has been so for some time, one of the exits it is trying to portray on the European level is shale gas, and it says that moving from coal to gas is the way forward. But at the same time it is fighting EU climate legislation on every front. Poland is clearly betting on shale gas and resisting with all its capacity EU legislation and an intake of renewables

In recent years, Gogolewski [10], [11] has rallied against the European Union's insufficiently fast transition to decarbonized economy and renewable energy and that this dependency on fossil fuels directly boosts Russia's capabilities to fund its war efforts in Ukraine:

> Many European banks and financial institutions are still, in one way or another, financing Russian fossil fuels and that money fuels Putin's illegal invasion of Ukraine. The connection is clear: fossil fuels (and

uranium) Europe buys from Russian companies. Those same companies not only fuel but also fund the Russian army, and thanks to some of the largest banks and investors in Europe, your money could be funding it. We need to expose and confront the European financial institutions still funding Russian fossil fuels and the war.

Beyond any doubt, Gogolewski's public positions are both anti-shale and anti-Russia in both energy deals and its military operations in Ukraine.

Another activist group that has remained vigorous since the anti-shale movements is Client Earth. This international environmental charity was targeted by Polish Treasury Minister Nikolaj Budzanowski for working against the public interests of the state with Polish conservative media going as far as to label the group as "eco terrorists" [12].

Client Earth's team has been vocal in their support for Ukraine and reducing Russia's energy dominance in Europe using fossil fuels. For example, on February 24, 2023, the group's [13] official X account published that:

Today marks the anniversary of Russia's invasion of Ukraine. Russia's war is a violation of Ukraine's sovereignty, which has devastated the lives of millions of innocent people. We stand in solidarity with the Ukrainian people.

The NGO's CEO Laura Clarke reposted the position as well. Clarke and the NGO profile asked for donations for the NGOs in Ukraine later the same day, arguing that despite the ongoing terrible conditions, activists and social organizations are still working with great courage in Ukraine. In 2022, Clarke was personally present at a meeting between the New Zealand foreign affairs staff and the UK Defence Select Committee where they discussed a range of issues, including Russia's invasion of Ukraine. Clarke has also retweeted other UK officials arguing in favour of the international community supporting Ukraine.

Another active public figure against shale gas has been Radoslaw Gawlik who had served as a vice minister in the cabinet of Jerzy Buzek and has seen turned into an environmentalist. Gawlik rallied against governmental efforts to suppress environmental NGOs who protested against shale gas development. He has also repeatedly participated in initiatives calling for the European authorities to impose a full embargo on Russian energy supplies such as the open letter to the EU Parliament from July 2024, signed by more than 100 leading international environmentalists [14]. While Gawlik's general attitude towards Russian energy supplies is undoubtedly negative, he had taken environmentalist positions that have jeopardized Polish infrastructure projects aimed at diminishing Russian dependency in transport, energy, trade, and others. One such example is the canal through Vistula Spit, which would reduce 100 kilometers from the journey that ships make towards the Polish port of Elblag and completely avoid going through the Russian-controlled Strait of Baltiysk. Gawlik criticized the project, arguing that "The billions of zloty which the government wants to sink into the Vistula spit, and to cement riverbeds under the pretext of creating river ways, should be instead devoted to fighting the drought, restoring natural retention, feeding groundwaters, river restoration as well as protecting wetlands and peat bogs" [15].

B. Bulgaria

The Bulgarian Council of Ministers approves a contract with the US company Chevron to explore potential shale gas fields in "Block 1 Novi Pazar" on 16.06.2011. The first protests and flash mobs against the decision come one month later – on 4th of August citizens gather in three Varna region municipalities to express their disagreement with shale gas development – in Vetrino, Valtchi Dol and Suvorovo [16]. On the next day, citizens gather to protest in front of the Bulgarian National Television's headquarters, requiring the broadcaster to screen the anti-shale movie Gasland. The movie is screened publicly in Varna on the 16th of August and the first national protest follows on the 1st of September [17]. The protest features a number of controversial claims, alleging earthquakes in the United Kingdom and land and water poisoning in Ecuador to have been caused by shale gas operations [17]. These are supported by the powerful Forthenature alliance of environmentalists and green NGOs, whose leaders to a sizeable extent overlap with the Green party leaders. Another large protest follows in the capital of Sofia on the 13th of September with the prime minister Borisov, Minister of economy, energy and tourism Traikov and minister of environment Karadzhova holding talks with anti-shale activists in the Council of ministers [18]. A well-publicized press conference on both topics features protest leaders Borislav Sandov, Angel Slavtchev and Mariana Hristova [18].

A number of national protests follows centred mostly in Sofia, Varna and Dobrich, which are accompanied with discussions, flash mobs and flurries of press releases, often citing allegations that had bordered conspiracy theories – such as small earthquakes at the Bulgarian seaside being caused by shale gas drilling. Mostly leftist, populist and socialist political parties such as ATAKA, the Bulgarian socialist party and RZS exploit the political cleavage and start calling for and filing legislation that bans shale gas exploration [19].

Following another flurry of protests and anti-shale events, the National Assembly [20] passed a decision that bans the full exploration and extraction of natural gas using hydraulic fracturing in Bulgaria.

Probably the most prominent organization against shale gas development in Bulgaria had been the "Citizens' initiative to ban shale gas exploration and extraction". On 24.01.2012 the Initiative gave a final press conference following a series of protests and a decision by Bulgaria's National Assembly to ban gas exploration and extraction using hydraulic fracturing. The press conference was led by the Initiative's leaders – Borislav Sandov, Angel Slavtchev, Mariana Hristova, Milen Stoyanov and Tatyana Koseva [21].

Another important opinion leader that needs to be mentioned is that of Mr. Toma Belev, who has been in the management team of Forthenature [22]. He has also sustainably taken positions against shale gas development and throughout the years has become a leading figure in Bulgarian environmentalism.

Analyzing the political standing of the above-mentioned opinion leaders reveals a diverse spectrum concerning Russia's involvement in supplying energy to Bulgaria and Europe, as well as the Russo-Ukrainian war.

Mr. Angel Slavtchev has joined a number of nationalist political parties between 2011 and 2025 and as of January 2025 he is member of the National Assembly of Bulgaria from the group of the nationalist political party Vazrazhdane. Mr. Slavtchev [23] has repeatedly laid his and his current party's views on important Russia-related foreign policy topics, for instance:

> We want a referendum for keeping the Bulgarian Lev, we want to stop supplying weapons to Ukraine, we want to restore economic relations with Russia and organize a referendum for exiting NATO.

In his last election campaign, Slavtchev [24] elaborates deeper on his vision for Bulgaria's involvement in the Russo-Ukrainian war:

> Enough of serving Euro-Atlantic values. We must serve Bulgarian values and the Bulgarian people, and build partnerships in the East and the West. There is no need to be service personnel at some embassy, we must work for Bulgaria. What is happening in Ukraine must stop immediately. Bulgaria must not send its soldiers into a conflict that is not ours. We at Vazrazhdane categorically oppose this scenario of sending Bulgarian soldiers to Ukraine, having a few coffins return and then having us put in this film, having us rise up against Russia too. We must not allow it. This is the plot of the directors from the West, including the USA, who are actively interfering, and our cadets are trump cards. We must stop this. We must not even send nurses there, we must not send weapons there. This is a fratricidal war and we have no place in it.

Slavtchev hasn't actively commented on the Russian energy dealings with Bulgaria throughout the last year since becoming a member of parliament, but his current party Vazrazhdane has been extremely active on this topic [25]. For instance, they claimed that the Bulgarian government is lying that Gazprom had stopped gas deliveries [25], they are the only ones who can successfully negotiate with Gazprom as noted by the party leader Kostadinov [26] and worsening relations with Gazprom would also worsen relations with other European countries such as Serbia and Hungary [27].

Borislav Sandov has had a notably different approach to Russian energy deals and the war. Shortly after resigning as a minister of the environment, Sandov [28], [29] had multiple interviews criticizing Gazprom for not fulfilling its contractual obligations to supply Bulgaria with natural gas. Sandov [28] is also highly critical of the Russian ambassador's diplomatic moves in Bulgaria at the time and the Bulgarian Socialist Party's views on rapprochement with Russia on the eve of the Russo-Ukrainian war:

> There is the Vienna Convention on Diplomatic Relations, and it must be observed. There is also the so-called principle of equality in diplomatic relations, and this is the reason why Russian diplomats were expelled from Bulgaria. The diplomatic mission of Russia exists, we have diplomatic relations and should maintain them, but when the Russian Federation engages in unprovoked military aggression on the territory of a sovereign state such as Ukraine, we cannot be subservient merely because we might rely on potentially lower gas prices. This would justify claims that Bulgaria is Russia's Trojan horse in Europe, and that cannot be a compromise position.

During his tenure as minister of Environment, Sandov [30] remains highly critical of shale gas development in Bulgaria and claims that the country has no viable deposits and shale gas cannot turn a profit without state subsidies. When pressed on whether such a position and moratorium on not only extracting, but also exploring for shale gas, serves the interests of Gazprom, Sandov deflects and claims that conventional gas supplier diversification is an easier and faster way to reduce dependence on Gazprom [30]. In the campaign for the 2024 parliamentary elections, Sandov [31] argued for maximizing support for Ukraine, including military, energy and giving a clear path for joining the European Union.

Toma Belev, who had served as deputy minister for the environment to Borislav Sandov, has expressed very similar positions concerning Russia to the latter. For instance, in 2024 he insisted on the next government to focus on joining Schengen, Eurozone, implementing a constitutional reform and aiding Ukraine in the war [32]. In 2022 Belev [22] had been criticizing the caretaker government at that time for not severing relationships with Gazprom and continuing to partner with Lukoil.

Tatyana Koseva, Milen Stoyanov and Mariana Hristova have been less active in public life since their successful lobbying for a moratorium on fracking. There are several recent interviews of Hristova [33], [34] with positions against natural gas development projects and indications that she has supported initiatives against intensifying EU-US relations in the area of trade [35].

C. Romania

Romania discovered non-conventional gas resources in Transylvania in the 1990s and has been one of the European countries investing significant hopes in shale gas development. The initial push for shale was led by the Democratic-Liberal government in 2012 which was however brought down shortly after initiating steps to explore shale gas deposits by the Social-Democrats with a motion of no confidence in April 2012. As the Social-Democrats came to power in 2012, the party's platform featured adamant opposition to shale gas extraction.

However, Victor Ponta's government opposition gradually softened and after a streak of negotiations with the USA state and non-state actors, Ponta [36] announced in January 2013 an almost complete reversal, arguing that shale gas development "should be considered as something positive". Widespread protests against shale gas started after several gas extraction rights were sold to Chevron in early 2013.

Throughout the spring of 2012, several thousands people marched repeatedly in the city of Barlad with protestors also involving representatives of the priesthood. Protests were renewed in the spring of 2013 again in Barlad but activists from other areas such as Bucharest, Constanta, galati and Buzau also attended. Protests spread quickly in April on the occasion of a global anti-fracking day. Protests escalated in intensity but had not turned violent until October 2013. In October, protestors and gendarmes clashed in Pungesti as Chevron moved to make first actual steps towards drilling, leading to fierce clashes and a dozen people being injured. Protests across Romania escalated in intensity with occasional violent outbursts until the end of 2014, expanding to block not only shale, but also conventional gas and oil projects.

Ultimately, the protests have been successful, initially toppling the Ungureanu government, suspending shale gas exploration in Pungesti, interrupting shale gas extraction from the Mosna-Alma Vii and forching Chevron to withdraw from Romania.

Romania's anti-shale movement had been highly decentralized and fragmented with massive grassroots campaigns joined by powerful local leaders in both municipal authorities, religious communities, entrepreneurs, and environmentalists. At the highest political level, politicians across a wide spectrum had expressed (and then sometimes reversed) anti-shale positions. However, most of the political leaders that had campaigned at some point against shale are firm supporters of the EU, NATO and Ukraine with highly critical opinion of Russian energy supplies and Russian military activities such as Traian Basescu [37] and Victor Ponta [38].

D. Discussion

The clearest evidence for a hypothetical involvement of Russian aligned state or non-state information warfare targeting the potential of Eastern European states developing shale gas is NATO's chief Rasmussen arguing that "I have met allies who can report that Russia, as part of their sophisticated information and disinformation operations, engage actively with so-called non-government organizations — environmental organizations working against shale gas — obviously to maintain European dependence on imported Russian gas" [39]. An anonymous NATO source concurred to Foreign Policy that there is a widespread concern among NATO members that "Russia could try to obstruct possible projects on shale gas exploration in Europe in order to maintain Europe's reliance on Russian gas" [39].

Johnson [39] also notes that Europe's decision making process on shale gas development had been more vulnerable to external information warfare "because environmental groups have more political power than in the United States and because higher population densities magnify the possible damaging effects of the drilling practice". In parallel, President Putin has repeatedly criticized the environmental impact of shale gas development, for instance by calling it "barbaric" [40] and arguing in length that it poses an insurmountable threat to the environment [41]:

> We all know that when fracking is used to produce shale gas the people in nearby towns no longer have water coming out of their taps but a blackish liquid that it would be difficult to call water. This poses a huge environmental problem. People always encounter these sorts of problems in hydrocarbon production.

Non-state Russian actors such as Gazprom's Alexey Miller have mirrored this position, arguing for an EU-wide ban on fracking as Zubrin [42] reports: "the production of shale gas is associated with significant environmental risks, in particular the hazard of surface and underground water contamination with chemicals applied in the production process". Zubrin [42] also reports on numerous Russian media outlets putting forward exaggerated reports on the risks of hydraulic fracturing with titles such as "Wrecking the Earth: fracking has grave radiation risks few talk about", "US fracking wells annually produce 280bn gallons of toxic waste destroying environment" and "Fracking dilemma: fresh water or cheap gas? The latter is not likely to happen" in RT.

Multiple Western analysts have also thrown serious doubt on the self-sufficiency of European environmental groups that sprang out of nowhere in countries such as Bulgaria and Ukraine in the early 2010s, which had until that moment shown no signs of organized and highly motivated environmentalism [39]. For instance, Brenda Shaffer [43] from Georgetown University argued that suddenly environmental movements started to target not only shale but also pipelines that would offer alternative gas transportation routes, "It's very concrete; it relates to both opposition to shale and also trying to block any alternative pipelines with environmental challenges, there is a lot of evidence here; countries like Bulgaria, Romania, Ukraine being at the vanguard of the environmental movement is enough for it to be conspicuous". Shaffer's words are echoed by those of Carstei [44] from the Atlantic Council, who points out that "all of a sudden, in societies that never did grassroots organization very well, you saw all these NGOs well-funded, popping up, and causing well-organized protests".

Although there have been some direct links between green NGOs' anti-shale campaigns and Russian state and non-state actors such as the ones described by former US ambassador to Lithuania Smith [45], their obscurity and relatively low number lead to suggestions that any external information warfare campaign would be far more elaborated and sophisticated than direct sponsorship or HUMINT. An overwhelming majority of the anti-shale activists are probably moved by genuine belief that hydraulic fracturing poses too many risks for the

environment and they are at the same time not aligning with Russia on any other topic as Johnson [39] points out:

> …much of Europe's anti-fracking movement is motivated by genuine environmental concerns, just as in the United States; much of that opposition was catalyzed by the controversial 2010 anti-shale documentary Gasland. There are fears about fracking's effect on groundwater and the link between fracking and increased seismic activity. France, for instance, banned fracking before Bulgaria. […] Environmental groups such as Greenpeace scoff at the NATO chief's allegations, saying that they oppose fracking for sound environmental reasons. What's more, there's little love lost between Greenpeace and Russia, because Moscow detained dozens of the group's green activists last year.

Yet, it is difficult to ignore that external state or non-state actors align too many pieces of the puzzle in a way that corresponds with a reflexive control campaign:

- the timing and coordination of the anti-shale campaigns in Bulgaria, Romania and Poland has been conspicuously similar;
- the common themes and messaging have largely ignored national contexts and concentrated on a cluster of environmental risks (water contamination, earthquakes and toxic fluids), lack of transparency (and supposed kickbacks for government officials) and foreign influence with fingers pointing towards the supposedly colonialist American capitalism;
- Russian media, political leadership and energy corporations have been active with exactly the same messaging and uniformly opposed hydraulic fracturing in Europe (while experimenting with the method in Russia)

Finally, as this article's research has proved, opponents of shale gas development do not share a uniform ideology and attitude towards Russia, which would have been evidence for a more direct external information or hybrid intervention. On the contrary, from today's point of view, most anti-shale campaigners are actually rallying behind Ukraine against Russia in the Russo-Ukrainian war while still trying to stop strategic energy projects that may reduce EU's dependency on Russian energy resources.

IV. Conclusions

More than a decade has passed since a wave of coordinated anti-shale activism has swept through Eastern Europe and terminated the initiatives of these countries to develop their own shale gas deposits and reduce dependency on fossil fuel imports. Despite the fact that many Western scholars have suspected that Russia was involved in supporting this environmental activism in order to cement its energy dominance over these states, rigorous research has uncovered too little direct links in the realm of finance, HUMINT, organization and media. This article suggests that any state or non-state Russian actors may have deployed the strategy of reflexive control in order to transmit specific information discrediting the utilization of hydraulic fracturing to a wide range of activists on the most basic environmental-moral level without interfering in these people's and organizations' attitude towards Russia. The textual analyses of statements of prominent anti-shale figures from Bulgaria, Romania and Poland proves that for the 10-15 years since the anti-shale wave they haven't clustered towards a pro-Russian position in any area, be it military, energy, environment, or else. On the contrary, their understanding, standing and activism on public policy and/or politics has branched out in different directions and probably most of them do not support Russia on any major public policy matter. This at least partially confirms the hypothesis for reflexive control application as this strategy aims to influence the adversary's decision-making without directly controlling the opponent but by transmitting information that is integrated in the decision-process.

Further research may investigate this matter in more EU countries and also add an analysis of the influence of US state and non-state actors who may have lobbied and/or tried to influence decision-making in the EU to facilitate the development of shale deposits – either from self-interest or as counteracting the hypothetical Russian campaign.

References

[1] T. Thomas. "Russia's reflexive control theory and the military". 2004. Journal of Slavic Military Studies, 17(2), 237–256. https://doi.org/10.1080/13518040490450529

[2] A. Vasara. "Theory of reflexive control: Origins, evolution and application in the framework of contemporary Russian military strategy". 2020. National Defense University

[3] A. Raskin.: Рефлексивное управление в социальных сетях. Informatsionnye Voĭny (in Russian). 2015. 35 (3) (Информационные войны ed.): 18–22. ISSN 1996-4544

[4] B. Mitrakiev and N. Dimitrov. "Russian Reflexive Control Campaigns Targeting Political Realignment of Ukraine's Democratic Allies: Critical Review and Conceptualization." 2024a. Information & Security: An International Journal,55no. 3:299-330.

[5] B. Mitrakiev and N. Dimitrov. "The Need for Emotional Cues Analysis in OSINT in Countering Reflexive Control Information Warfare Campaigns: A Critical Review and Reconceptualization." 2024b. Information & Security: An International Journal, 55 no.3:275-298.

[6] T. Tagarev and P. Fluri. "From Civil-Military Relations to Resilience: The Fifth Wave of Strengthening Democracy through Research and Education". 2025. Available: https://procon.bg/system/files/24.1.06_democratic_resilience.pdf [Accessed February 11, 2025]

[7] US Energy Information Administration. "World Shale Gas Resources: An Initial Assessment of 14 Regions Outside the United States". April, 2011. Available: https://www.eia.gov/analysis/studies/worldshalegas/pdf/fullreport.pdf [Accessed February 9, 2025]

[8] Bankwatch. "EIB restricts – but does not eliminate – coal and other fossil fuel lending". July, 2013. Available: https://bankwatch.org/press_release/eib-restricts-but-does-not-eliminate-coal-and-other-fossil-fuel-lending [Accessed February 9, 2025]

[9] E. King. "Polish government accused of gagging anti-fracking groups". March, 2013. Available: https://www.climatechangenews.com/2013/03/22/polish-govement-accused-of-stifling-national-shale-gas-debate/ [Accessed February 9, 2025]

[10] K. Gogolewski. "ECB's broken promise on bond decarbonisation creates climate gap". July, 2023. Available:

https://greencentralbanking.com/2023/07/26/ecbs-corporate-bond-decarbonisation/ [Accessed February 9, 2025]

[11] K. Gogolewski. "Is your money funding Putin's war machine?". April, 2022. Available: https://www.greenpeace.org/international/story/53254/european-money-finance-funding-putins-war-machine/ [Accessed February 9, 2025]

[12] A. Neslen. "Poland accused of creating climate of fear for environemntal campaigners" October, 2012. Available: https://www.theguardian.com/environment/2012/oct/30/poland-climate-fear-environmental-campaigners [Accessed February 11, 2025]

[13] Client Earth. "Today marks the anniversary of Russia's invasion of Ukraine. Russia's war is a violation of Ukraine's sovereignty, which has devastated the lives of millions of innocent people. We stand in solidarity with the Ukrainian people." February, 2023. Available: https://x.com/ClientEarth/status/1629013230696771585 [Accessed February 11, 2025]

[14] Razom we stand. "Open letter: 1st EU Parliament resolution on embargo of russian gas by the end of 2024". July, 2024. Available: https://razomwestand.com/open-letter-1st-eu-parliament-resolution-on-embargo-of-russian-gas-by-the-end-of-2024/ [Accessed February 11, 2025]

[15] K. Cibor. "Pieniadze wpuszczone w kanal, zamiast walki z susza". May, 2020. Available: https://www.greenpeace.org/poland/aktualnosci/28546/pieniadze-wpuszczone-w-kanal-zamiast-walki-z-susza/ [Accessed February 11, 2025]

[16] Darik, "Flash mobs in three places in Varna against the shale gas development". August, 2011a. Available: https://dariknews.bg/regioni/varna/flashmob-na-tri-mesta-vyv-varnensko-zaradi-dobiva-na-shistov-gaz-757686 [Accessed February 3, 2025]

[17] Forthenature. "National protest against exploration and extraction of shale gas in Bulgaria". August, 2011. Available: https://forthenature.org/actions/278 [Accessed February 3, 2025]

[18] Darik. "A protest against shale gas is being organized for next month". September, 2011b. Available: https://dariknews.bg/novini/biznes/protest-sreshtu-dobiva-na-shistov-gaz-u-nas-sledvashtiq-mesec-783019 [Accessed February 3, 2025]

[19] B. Rilska. "Following a recommendation by Borisov, RZS and independent members of parliament from Ataka file legislation that bans the extraction of shale gas". November, 2011. Available: https://www.dnevnik.bg/bulgaria/2011/11/23/1210402_po_zaruka_na_borisov_rzs_i_nezavisimi_ot_ataka_vnesoha/ [Accessed February 3, 2025]

[20] National Assembly of Bulgaria. "Decision for banning the hydraulic fracturing technology for exploring and extracting gas and oil in the Republic of Bulgaria". January, 2012. Available: https://www.parliament.bg/bg/desision/ID/13824 [Accessed February 3, 2025]

[21] Econ.bg, "Pressconference given by Citizens' initiative to ban shale gas exploration and extraction". January, 2012. Available: https://econ.bg/%D0%A1%D1%8A%D0%B1%D0%B8%D1%82%D0%B8%D1%8F/%D0%9F%D1%80%D0%B5%D1%81%D0%BA%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D0%B8%D1%8F-%D0%BD%D0%B0-%D0%93%D1%80%D0%B0%D0%B6%D0%B4%D0%B0%D0%BD%D1%81%D0%BA%D0%B0-%D0%B8%D0%BD%D0%B8%D1%86%D0%B8%D0%B0%D1%82%D0%B8%D0%B2%D0%B0-%D0%B7%D0%B0-%D0%B7%D0%B0%D0%B1%D1%80%D0%B0%D0%BD%D0%B0-%D0%BD%D0%B0-%D0%BF%D1%80%D0%BE%D1%83%D1%87%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F%D1%82%D0%B0-%D0%B8-%D0%B4%D0%BE%D0%B1%D0%B8%D0%B2%D0%B0-%D0%BD%D0%B0-%D1%88%D0%B8%D1%81%D1%82%D0%BE%D0%B2-%D0%B3%D0%B0%D0%B7_l.a_i.374722_at.2.html [Accessed February 3, 2025]

[22] T. Belev. "There won't be any gas but the gas that won't be will at least be Russian". August, 2022. Available: https://darik.bg/nakraa-gaz-nama-da-ima-no-pone-toa-gaz-deto-go-nama-ste-e-ruski-i-oste-ot-feisbuk [Accessed February 9, 2025]

[23] A. Slavtchev. "Vazrazhdane will not negotiate with GERB". November, 2024a. Available: https://www.bgonair.bg/a/218-izbori-2024/363429-angel-slavchev-vazrazhdane-nyama-da-pregovarya-s-gerb [Accessed February 4, 2025]

[24] A. Slavtchev. "No Bulgarian soldiers will go in Ukraine". May, 2024b. Available: https://vazrazhdane.bg/%D0%B0%D0%BD%D0%B3%D0%B5%D0%BB-%D1%81%D0%BB%D0%B0%D0%B2%D1%87%D0%B5%D0%B2-%D0%B1%D0%B5%D0%B7-%D0%B1%D1%8A%D0%BB%D0%B3%D0%B0%D1%80%D1%81%D0%BA%D0%B8-%D0%B2%D0%BE%D0%B9%D0%BD%D0%B8%D1%86%D0%B8-%D0%B2%D0%B2/ [Accessed February 4, 2025].

[25] Vazrazhdane. "The government is lying that Russia stopped gas supplies in order to buy it from intermediaries – they should resign". May, 2022. Available: https://glasove.com/novini/vazrazhdane-pravitelstvoto-lazhe-che-rusiya-ni-e-spryala-gaza-za-da-go-kupuva-prez-posrednik-ostavka [Accessed February 4, 2025]

[26] K. Kostadinov. "Only Vazrazhdane can successfully negotiate with Gazprom". August, 2022. Available: https://bnr.bg/horizont/post/101697355/kostadinov-samo-vazrajdane-moje-da-vodi-uspeshni-pregovori-s-gazprom [Accessed February 4, 2025]

[27] Vazrazhdane. "Asen Vasilev is attempting to extort Gazprom". October, 2023. Available: https://fakti.bg/bulgaria/827368-vazrajdane-asen-vasilev-iska-da-reketira-gazprom [Accessed February 4, 2025]

[28] B. Sandov. "I see no reason to negotiate with Gazprom". July, 2022a. Available: https://bntnews.bg/news/borislav-sandov-db-az-ne-vizhdam-kakvi-pregovori-mozhe-da-vodim-s-gazprom-1201991news.html [Accessed February 9, 2025]

[29] B. Sandov. "The caretaker government has no business dealing with Gazprom". August, 2022b. Available: https://btvnovinite.bg/predavania/tazi-sutrin/sandov-za-otnoshenijata-s-gazprom-tova-ne-e-rabota-na-sluzhebnija-kabinet.html [Accessed February 9, 2025]

[30] B. Sandov. "Sandov in the Day with V. Dremdzhiev". January, 2022c. Available: https://www.youtube.com/watch?v=WnRQmpAPTV8 [Accessed February 9, 2025]

[31] B. Sandov. "Maximum support for Ukraine, the aggressor will soon collapse economically". May, 2024. Available: https://zelenodvizhenie.bg/borislav-sandov-maksimalna-podkrepa-za-ukrayna-agresorat-skoro-shte-se-srine-ikonomicheski/ [Accessed February 9, 2025]

[32] T. Belev. "It is more important what Bulgaria's foreign policy would be rather than who the foreign minister will be". February, 2024. Available: https://bnr.bg/horizont/post/101949096/toma-belev-vajno-e-kakva-shte-e-vanshnata-politika-na-balgaria-a-ne-koi-shte-e-ministar [Accessed February 9, 2025]

[33] M. Hristova. "Costs and benefits of developing oil and gas projects in Dobrudzha". September, 2014. Available: https://nova.bg/news/view/2014/09/02/84962/%D0%BF%D0%BE%D0%BB%D0%B7%D0%B8%D1%82%D0%B5-%D0%B8-%D0%B2%D1%80%D0%B5%D0%B4%D0%B8%D1%82%D0%B5-%D0%BE%D1%82-%D0%BF%D1%80%D0%BE%D1%83%D1%87%D0%B2%D0%B0%D0%BD%D0%B5%D1%82%D0%BE-%D0%B8-%D0%B4%D0%BE%D0%B1%D0%B8%D0%B2%D0%B0-%D0%BD%D0%B0-%D0%B3%D0%B0%D0%B7-%D0%B8-%D0%BD%D0%B5%D1%84%D1%82-%D0%B2-%D0%B4%D0%BE%D0%B1%D1%80%D1%83%D0%B4%D0%B6%D0%B0/ [Accessed February 9, 2025]

[34] M. Hristova. "A referendum is enough to stop an investment initiative". February, 2019. Available: https://bnr.bg/post/101078804/mariana-hristova-referendumat-e-dostatachen-za-da-spre-edno-investicionno-namerenie?fbclid=IwY2xjawIV3WZleHRuA2FlbQIxMQABHUGk2i7TvpUMe9xtVj4Ic8Ke_KR274FHPFrh3md7t6_-YbUWNFtxzGvZhQ_aem_wIw5qWMVeEviCk40dwM9IQ [Accessed Februaary 9, 2024]

[35] A-specto. "Mariana Hristova: our food is poisonous". April, 2016. Available: https://a-specto.bg/interviuta/mariana-hristova-hranata-ni-e-otrova [Accessed February 9, 2025]

[36] C. Pantazi. "Cum s-a schimbat pozitia USL fata de gazele de sist. De la motiune de cenzura pina la idee care trebuie tratata "serios pozitiv"". January, 2013. Available: https://hotnews.ro/cum-s-a-schimbat-pozitia-usl-fata-de-gazele-de-sist-de-la-motiune-de-cenzura-pina-la-idee-care-trebuie-tratata-serios-pozitiv-613753 [Accessed February 11, 2025]

[37] A. Ventsel. "Traian Basescu: Russia is a clear threat to all black sea states". April, 2020. Available: https://icds.ee/en/traian-basescu-russia-is-a-clear-threat-to-all-black-sea-states/ [Accessed February 11, 2025]

[38] V. Ponta. "How can Romania help Ukraine? Y helping herself! A vision for a new integrated territorial investment program". September, 2023. Available: https://www.euractiv.com/section/global-europe/opinion/how-can-romania-help-ukraine-by-helping-herself-a-vision-for-a-new-integrated-territorial-investment-program/ [Accessed February 11, 2025]

[39] K. Johnson. "Russia's quiet war against European fracking". June, 2014. Available: https://foreignpolicy.com/2014/06/20/russias-quiet-war-against-european-fracking/ [Accessed February 9, 2025]

[40] S. Meredith. "Russia's Putin says shale oil technologies are barbaric". 2019. Available: https://www.cnbc.com/2019/11/20/russias-putin-says-shale-oil-technologies-are-barbaric.html [Accessed 13.02.2025]

[41] V. Putin. "Speech at the plenary session of the Third International Arctic Forum The Arctic – A territory of dialogue". September, 2013. Available: http://en.kremlin.ru/events/president/transcripts/19281 [Accessed 13.02.2025]

[42] R. Zubrin. "Putin's anti-fracking campaign". May, 2014. Available: https://www.nationalreview.com/2014/05/putins-anti-fracking-campaign-robert-zubrin/ . [Accessed February 9, 2025]

[43] B. Shaffer. "Pipeline problems". March, 2014. Available: https://www.foreignaffairs.com/articles/ukraine/2014-03-11/pipeline-problems [Accessed 13.02.2025]

[44] M. Carstei. "Carstei on Russia's War against fracking". June, 2014. Available: https://www.atlanticcouncil.org/insight-impact/in-the-news/carstei-on-russias-war-against-fracking/ [Accessed 13.02.2025]

[45] K. Smith. "Unconventional gas and European security: politics and foreign policy of fracking in Europe". 2012. Available: https://www.usubc.org/site/files/Unconventional_Gas_and_European_Security.pdf [Accessed 13.02.2025]

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 201-207

Examining the Impact of Image Augmentation on Object Detection and Classification to Improve Performance of Situational Awareness Systems

Svilen Neykov
Bulgarian Defence Institute "Prof. Tsvetan Lazarov"
Sofia, Bulgaria
ORCID: 0009-0005-3975-2781
WoS: KEH-5558-2024
svilen@nkv.me

***Abstract*—Situational Awareness (SA) and Artificial Intelligence (AI) go hand-in-hand in future applications, be that civilian applications, disaster relief or especially in the military domain. There, providing the most information, as quickly and as precisely as possible is crucial to completion of the given mission both in acquiring and denying the materiel and personnel. Object detection and classification are integral parts of this and will be the cornerstone in the coming years for developments and advances in civilian and military life. it is vital that these systems can operate in all weather conditions and be able to discern subtle differences in the observed objects, without relying on additional equipment.**

Keywords*— *Artificial Intelligence, Object Detection, Situational Awareness.

I. INTRODUCTION

There are various fields where AI algorithms may enhance both situational awareness and decision-making speed and precision. Such may include disaster mitigation and remediation, search and rescue operations, vehicle and machinery operation, etc. Even more in the military where AI has not yet entered with its full force and hype. One key area here can be Target Acquisition and Friend-Foe identification, especially in theatres where similar materiel is used and there is a lack of training material for the algorithms. Here state-of-the-art Object detection algorithms come into play. In this paper one such algorithm is examined, both in a pre-trained and trained on a very limited dataset, as well as using augmentation techniques to see the impact it can have on results.

II. MATERIALS AND METHODS

A. Object Detection Algorithms

The human is a visual animal, most of the information our brains process is visual, and we have built the world around us based on this. Visual cues, movement, patterns and imperfections are a small part of the information we can process naturally. However, we are prone to boredom, tiredness, loss of vision due to various medical, psychological and environmental reasons. Here enters the digital eye. Sensors, optics that can be designed to be vastly superior to the human eye. They can process information faster, can operate in various environments and weather conditions, and work in light-bands impossible for the human eye. Thus, computer vision is introduced.

Computer Vision has wide application in almost every aspect of the modern world. Industrial applications such as defect monitoring, assembly verification, safety checks, maintenance, etc. Research applications such as identification of cell types, quality checks of drug crystalline structures, etc. In everyday life such as vehicle monitoring for toll collection, CCTV monitoring for law-enforcement, disaster prevention and relief, access verification for home and office spaces and so on.

One of the greatest fields where Computer Vision, can be used is n the military domain. Here information is vital. Having as much information as possible and being able to process this information as fast as possible and as accurately as possible provides an edge for you and your allies and puts the opposing forces at a measurable disadvantage. One of the major computer vision aspects is Object Detection and Classification. Traditionally object detection has utilized sliding windows which select regions of the image, but it is very hard to find the optimal number

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8491
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

of these windows. The traditional methods rely heavily on manually created features, which struggle with accuracy and robustness when viewing diverse objects and possess complex backgrounds. These features also have one additional flaw - they are not universal, this translates to poor multi-domain performance and high complexity and time-consumption in region selection. With Deep Learning (DL) booming in the industry, object detection utilizing DL has vastly improved and surpassed traditional object detection methods. DL-based algorithms use very intricate and strictly hierarchical architectures, these enable the training of more complex features. Also, owing to the significant learning capabilities of convolutional neural networks (CNNs) feature can be better represented than traditional methods. This in turn raises significantly the robustness and eliminates the manually created features. [1]

B. Situational Awareness

Situational Awareness refers to being aware of one's surroundings and reacting appropriately to identified stimuli. SA is important in all aspects of life, industrial production, emergency and disaster response, infrastructure monitoring, etc. It is however vitally important in the Military domain. SA is viewed as an integral part of the Modern Command and Control (C2) system alongside planning, tasking and control. Recently, a lot of research has been done on crisis assessment [2] [3], as well as C2 system models [4]. For a field commander or a chief of an emergency response center being aware of all possible actors on the field, their identification, intention, status and movement vector is crucial in developing a complete picture. This picture directly impacts the plan-making and decision process used. The SA and decision-making model which here we can use is based on the one proposed by Munir, Arslan, Alexander Aved, and Erik Blasch. Here we can see clearly 3 Levels of SA: Level 1 - Perception: here are listed items pertaining to identifying the presence of an object. Level 2 - Comprehension: here we can see the linking of the objects from level 1 into a more complete picture, understanding their relation and significance through the lens of the operators' objectives. Level 3 - Projection: here we can find the projection of possible future actions of the identified objects and possible ways to perform actions in a way that is outside of their SA. When discussing this model, we can see that the work presented is combining Level 1 and Level 2, as apart from identifying if there is an object, it tries to identify if this object is in the blue or red team, and so it enhances the understanding of the objects after identifying them. [5]

C. Target Acquisition and Friend-Foe Identification

Target Acquisition in the post-Cold War era refers to Identification and Assessment of capabilities, assets and identities of formations, systems and materiel in general. This is especially important in Identifying and Acquiring High Value Targets and High Pay-Off Targets, which when neutralized would provide a significant contribution to the success of the friendly/blue team forces. This process requires a significant structure model to have a robust process and possess the ability to choose the high-value targets (HVTs) and/or high-priority targets (HPTs). To facilitate this a friend-for identification system can also be used. This would lessen the computational burden by sifting through all the initial contacts and marking blue (friendly) forces beforehand. This type of system however has its limitations, as only friendly/blue forces may be positively identified, however they may not be able to respond, due to various reasons, some of which are malfunctions, lack of Identification friend or foe (IFF) equipment and so on. IFF is a tool within the broader military action of combat identification (CID), the characterization of objects detected in the field of combat sufficiently accurately to support operational decisions. The broadest characterization is that of friend, enemy, neutral, or unknown. CID not only can reduce friendly fire incidents but also contributes to overall tactical decision-making. [6]

Here is where additional Identification, mainly visual can have a massive positive effect and Artificial Intelligence, especially object detection and classification algorithms has its place.

III. Results and Discussion

A. Setup

Utilizing a state-of-the-art algorithm, we can try to assess the impact of image augmentations, epoch number, model size and the use of pre-trained models when using a small dataset of publicly available images of military materiel. The main goal is to identify Blue and Red forces, ie. Friendly and Foe tanks.

1) The Model: When speaking about DL based object detection one of the leading CNN based models that exist is You Only Look Once (YOLO). Based on the human way of glancing at an image and instantly identifying the objects in the image, their locations and interactions. This allows humans to perform complex tasks with little to no conscious thought. YOLO looks at the whole image and makes predictions based on global context in the image, as well as performing them with a single evaluation, unlike R-CNNs which require numerous evaluations for a single image. [7]

Here we use the latest available YOLOv8 which is an evolution on the previous iterations with greater robustness and enhanced performance, as seen in Figure 1.

Apart from selecting the proper Model, we need to select the size of the model. For the following experiments 3 sizes were selected, in order to explore if and how the number of parameters influence accuracy with small datasets. Here we will use the n, s and m variants. Also, the pre-trained weights that will be used are based on the Common Objects in Context (COCO) dataset, where the attained performance is shown in Table 1.

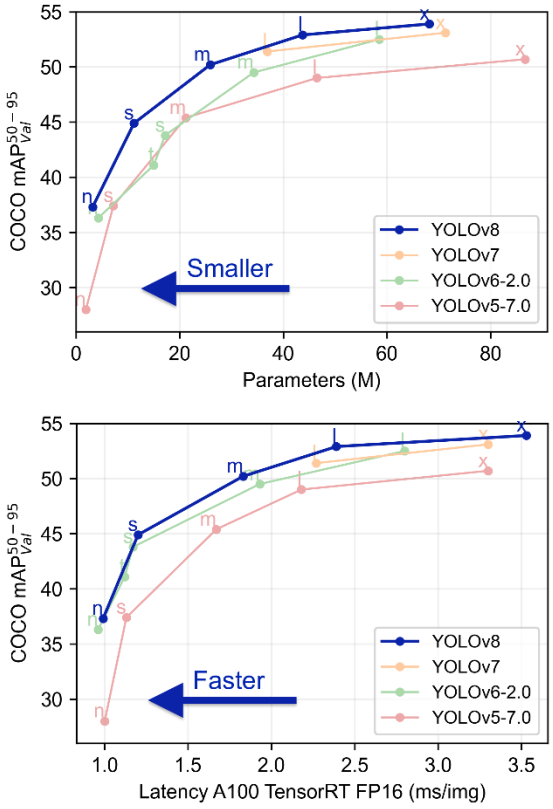


Fig. 1. Comparison of YOLO performance across versions [8]

TABLE 1 COMPARISON OF YOLO MODEL SIZES [8]

Model	Size (pixels)	mAPval 50-95	Params (M)
YOLOv8n	640	37.3	3.2
YOLOv8s	640	44.9	11.2
YOLOv8m	640	50.2	25.9

2) The Dataset: One of the biggest challenges in the Military domain regarding the use of AI techniques is the relative scarcity of available training data, as well as the quality of the data. A large number of the available photos for military materiel is from the official channels from the governments or trade shows where the equipment is shown. These bring the problem too clean a data point, as the photos usually are in perfect lighting conditions, no weather effects at all, as they are taken in hangers or pavilions. These can be used in training, but when a model trained of this data is used in real worlds environments it may struggle with various artefacts, weather conditions, lens distortion and so on. However, even a small dataset is preferable to a non-existent one, so the one used compromises of 1069 images of tanks. These are prepared for You Only Look Once v8 (YOLOv8) by the Roboflow platform and separated in a 70/20/10 split for training, validating and testing respectively. The sample is limiting in one more aspect, as the goal is not only to see the performance of object detection, but also for classification of friendly and foe forces, where both sides can utilize the same or almost the same model of tank. For example, the upgraded Soviet era T-72B3/4 and the Czech version T-72M4. Some examples are shown in Figures 2 and 3.



Fig. 2. Russian T-72B4



Fig. 3. Czech T-72M4

3) The Augmentations: The image augmentation techniques used here are focused mainly on simulating real-world conditions such as distortions and weather effects, as well as the already standard partial images, mosaic distortion, etc. These are implemented through the Albumentations [9] add-on for Ultralytics YOLOv8. The used augmentations include the following:

- ImageCompression
- RandomFog
- RandomRain
- RandomShadow
- RandomSnow
- RandomSunFlare

As well as the standard in-built MixUp augmentations. Examples of the augmented images are shown in Figures 4 and 5.



Fig. 4. Training batch of images with random weather effects

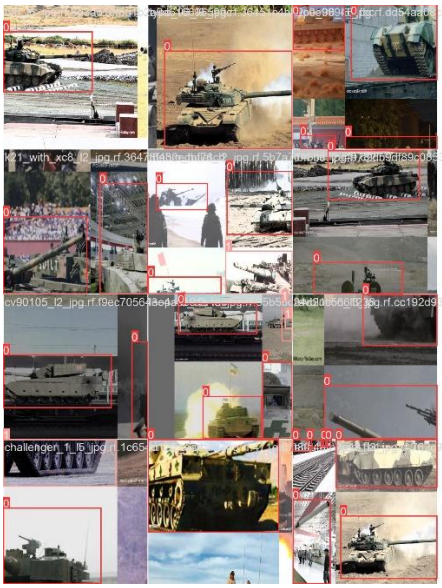
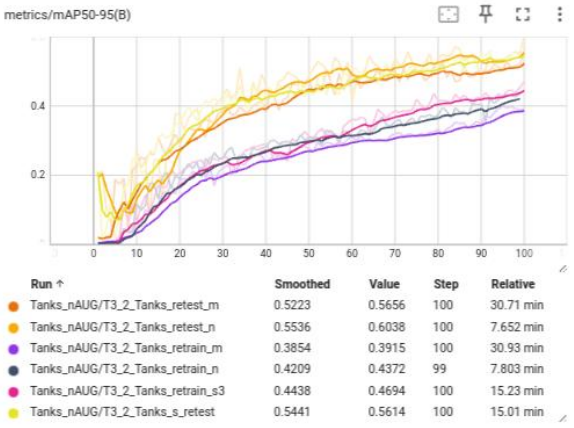


Fig. 5. Training batch of images without random weather effects

B. Results

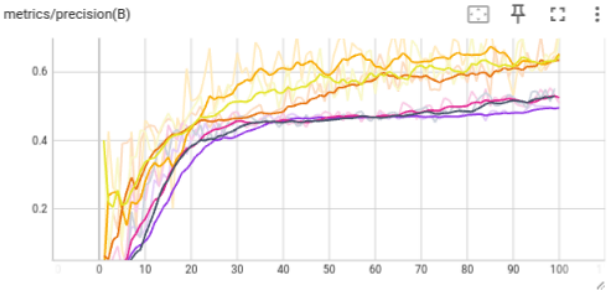
We will experiment with both re-training of the models and using pre-trained weights on our dataset, as well as the impact of a longer training period (100 epochs vs 200 epochs) and the effect of the augmentations on the accuracy and recall.

1) Re-training versus pre-trained weights: The first variable we will look at is if re-training the models with the very limited available dataset will provide a benefit, or the pretrained models will be able to transfer their domain knowledge to an unknown domain well enough. This has been validated for all three sizes of the Model. See Figures 6, 7 and 8.



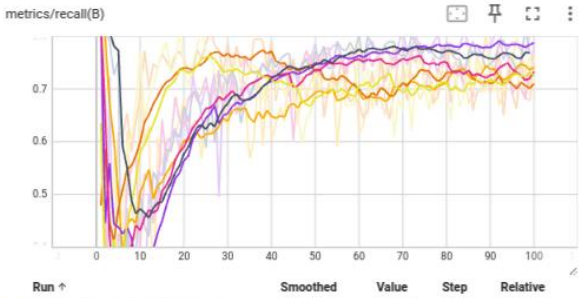
Run	Smoothed	Value	Step	Relative
Tanks_nAUG/T3_2_Tanks_retest_m	0.5223	0.5656	100	30.71 min
Tanks_nAUG/T3_2_Tanks_retest_n	0.5536	0.6038	100	7.652 min
Tanks_nAUG/T3_2_Tanks_retrain_m	0.3854	0.3915	100	30.93 min
Tanks_nAUG/T3_2_Tanks_retrain_n	0.4209	0.4372	99	7.803 min
Tanks_nAUG/T3_2_Tanks_retrain_s3	0.4438	0.4694	100	15.23 min
Tanks_nAUG/T3_2_Tanks_s_retest	0.5441	0.5614	100	15.01 min

Fig. 6. mAP50 for Re-train vs Pre-trained



Run	Smoothed	Value	Step	Relative
Tanks_nAUG/T3_2_Tanks_retest_m	0.6357	0.6449	100	30.71 min
Tanks_nAUG/T3_2_Tanks_retest_n	0.6534	0.7282	100	7.652 min
Tanks_nAUG/T3_2_Tanks_retrain_m	0.4949	0.4986	100	30.93 min
Tanks_nAUG/T3_2_Tanks_retrain_n	0.5305	0.5523	99	7.803 min
Tanks_nAUG/T3_2_Tanks_retrain_s3	0.5257	0.5088	100	15.23 min
Tanks_nAUG/T3_2_Tanks_s_retest	0.6472	0.7072	100	15.01 min

Fig. 7. Precision for Re-train vs Pre-trained



Run	Smoothed	Value	Step	Relative
Tanks_nAUG/T3_2_Tanks_retest_m	0.7101	0.7466	100	30.71 min
Tanks_nAUG/T3_2_Tanks_retest_n	0.7412	0.7624	100	7.652 min
Tanks_nAUG/T3_2_Tanks_retrain_m	0.7879	0.8045	100	30.93 min
Tanks_nAUG/T3_2_Tanks_retrain_n	0.7687	0.7662	99	7.803 min
Tanks_nAUG/T3_2_Tanks_retrain_s3	0.7326	0.7824	100	15.23 min
Tanks_nAUG/T3_2_Tanks_s_retest	0.7253	0.6994	100	15.01 min

Fig. 8. Recall for Re-train vs Pre-trained

2) Impact of number of epochs: The second variable we will look at is the number of epochs and it's impact, mainly to see if spending more machine time will improve significantly the results. This has been validated for all three sizes of the Model. Also we will look at the time it

took to complete the runs with a single Nvidia RTX 4070 Super card. See Table 2.

TABLE 2 COMPARISON OF EPOCH NUMBER AND TIME FOR COMPLETION OF RUNS

Model	mAP50	mAP50-95	Precision	Recall	Time
pre-trained N 100	0.7735	0.6038	0.7282	0.7624	7.652 min
pre-trained N 200	0.7437	0.5892	0.6463	0.7817	15.22 min
pre-trained S 100	0.7218	0.5614	0.7072	0.6994	15.01 min
pre-trained S 200	0.7443	0.5917	0.7248	0.6991	30.81 min
pre-trained M 100	0.7236	0.5656	0.6449	0.7466	30.71 min
pre-trained M 200	0.7162	0.5638	0.6429	0.7389	59.84 min

3) Impact of Augmentations: The third variable we will look at is the augmentations in order to see if and how adding them changes the behavior of the training and the results. This has been validated for all three sizes of the Model but only for 100 epochs. See Figures 9 and 10, and Table III.

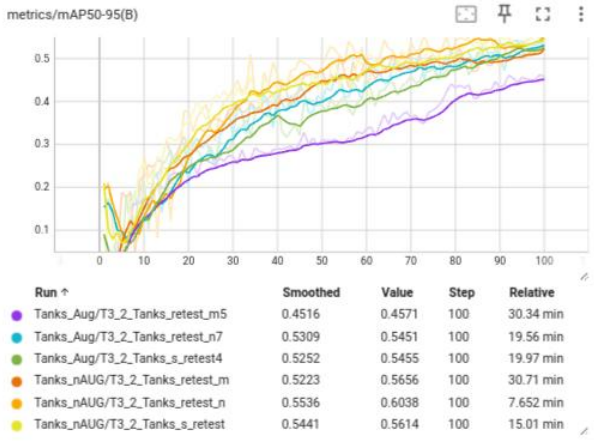


Fig. 9. mAP50-95 for all 3 models with and without augmentations

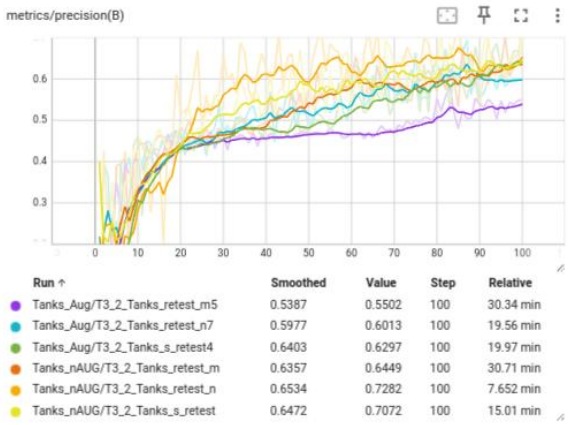


Fig. 10. Precision for all 3 models with and without augmentations

TABLE 3 COMPARISON OF AUGMENTATIONS IMPACT AND SIZE OF MODEL

Model	mAP50	mAP50-95	Precision	Recall	Time
Aug/YOLOv8m	0.6001	0.4571	0.5502	0.7223	30.34 min
Aug/YOLOv8n	0.6996	0.5451	0.6013	0.7778	19.56 min
Aug/YOLOv8s	0.6965	0.5455	0.6297	0.7033	19.97 min
No Aug/YOLOv8m	0.7236	0.5656	0.6449	0.7466	30.71 min
No Aug/YOLOv8n	0.7735	0.6038	0.7282	0.7624	7.652 min
No Aug/YOLOv8s	0.7218	0.5614	0.7072	0.6994	15.01 min

C. Pre-Training vs. Re-Training

The comparison given here shows significant performance disparities. The COCO dataset pre-trained YOLOv8n model achieved 68.2% mAP50 (Mean Average Precision) on test data, compared to 52.4% for the re-trained equivalent – a 30.2% relative improvement. This shows the importance of transfer learning in military AI applications where annotated datasets remain scarce. The pre-trained models' ability to generalize from civilian to military vehicles, this suggests latent feature representations applicable across domains.

D. Model sizes

The size analysis shows counterintuitive results – the YOLOv8s variant outperformed larger (m) and smaller (n) counterparts when using pre-trained weights, achieving 72.1% mAP50 versus 68.9% (m) and 68.2% (n). This suggests that intermediate model complexity optimally balances parameter count and generalization capability for the given dataset size. The inverse relationship between model size and performance in limited-data scenarios highlights the risk of over-parameterization in military AI systems where training data acquisition faces operational constraints.

E. Epochs and Efficiency

Here we see non-linear returns on epoch extension. Doubling epochs from 100 to 200 yielded only 2.8% mAP50 improvement for YOLOv8s, while increasing training time by 87%. This diminishing return suggests practical optimization thresholds exist based on operational urgency and resource availability. By using consumer-grade hardware the study demonstrates feasibility for field-deployable training systems.

Energy efficiency metrics derived from training times and hardware specifications suggest potential for edge-computing implementations. The YOLOv8n model's 2.7-hour training time at 100 epochs versus YOLOv8m's 5.1-hour duration provides commanders with flexibility in model selection based on mission requirements. These findings challenge assumptions about needing specialized hardware for military AI implementations, supporting decentralized training paradigms.

F. Strategies and Trade-Offs

The Albumentations framework implemented six environmental degradation techniques: image compression (simulating transmission artifacts), random fog, rain, shadow, snow, and sun flare. Quantitative analysis reveals a 4.2% decrease in mAP50-95 for YOLOv8s with augmentations enabled, contrasted with a 7.1% recall improvement in foggy conditions. This precision-recall trade-off suggests augmentation strategies must align with mission priorities—surveillance systems prioritizing threat detection may accept lower precision for higher recall, while targeting systems require inverse optimization.

Qualitative analysis of activation maps shows weather augmentations forcing feature focus on structural vehicle components rather than surface textures. This shift improves invariance to environmental conditions but reduces discrimination capability for visually similar variants. The snow augmentation proved particularly detrimental, degrading mAP50 by 9.3% compared to non-augmented baseline. These findings underscore the need for mission-specific augmentation pipelines rather than universal application.

G. Friend-Foe Identification Challenges

The dataset's composition of visually similar adversarial vehicles (Russian T-72B4 vs. Czech T-72M4) tests classification boundaries under operational constraints. Baseline performance without augmentations achieved 84.6% friend-foe accuracy, dropping to 79.1% with weather augmentations enabled. This 5.5% decrease highlights the vulnerability of visual identification systems to environmental degradation, necessitating multi-modal sensor fusion for reliable combat identification.

Error analysis reveals confusion in side-profile views where variant-specific modifications (explosive reactive armor configuration, storage boxes) become occluded. Augmentations exacerbating edge blurring (compression, fog) disproportionately impacted these cases, suggesting terrain-specific augmentation strategies. For urban combat scenarios with frequent partial occlusions, targeted occlusion augmentations during training may improve robustness beyond generic weather effects.

IV. Conclusions

The integration of AI into military SA systems represents a critical next step in modern defence technology. Through this study we explore the efficacy of image augmentation techniques in enhancing object detection and classification accuracy for friend-foe identification. Key findings show that pre-trained models consistently outperform re-trained counterparts, smaller model architectures demonstrate superior adaptability to limited datasets, and strategic image augmentations improve recall at the expense of precision. Computational efficiency analysis shows diminishing returns with increased training epochs. Weather-based augmentations introduce trade-offs that vary depending on the size of the models used.

These insights show that it is vital to balance the model complexity, training strategies, and augmentation selection to optimize performance where data is scarce, especially in military applications.

A. Situational Awareness Hierarchy

The three-level SA model provides a framework for evaluating AI systems. Current systems are focused on Level 1 (object detection) and Level 2 (contextual classification), with friend-foe identification bridging these levels through semantic understanding. Decision making in the military domain requires not only detection accuracy, but contextual interpretation – the ability to distinguish between Fig. 2 and Fig. 3, this carries different tactical implications than generic vehicle detection.

This hierarchical understanding becomes especially complex when having in mind adversarial deception tactics. The inclusion of near-identical vehicle models from opposing forces in the dataset tests the system’s ability to discern subtle visual differences – a capability crucial for preventing fratricide and ensuring target validity. When the focus are these edge cases the study addresses this critical gap in practical military AI applications.

B. Limitations and Future Research Directions

The study's primary limitation stems from its 1,069-image dataset—orders of magnitude smaller than commercial computer vision benchmarks. Performance disparities between pre-trained and re-trained models (15.8% mAP50 difference) directly correlate with this data scarcity. Future work must address military data acquisition challenges through synthetic data generation using game engines or 3D modeling, potentially combined with limited real-world captures.

The dataset's focus on static vehicle imagery neglects motion blur and dynamic engagement scenarios. Incorporating temporal sequences and multi-view captures could improve model robustness to realistic battlefield conditions. Additionally, the absence of civilian vehicles in the dataset limits understanding of false positive rates in

complex environments—a critical consideration for urban operations.

Where the study can be taken is with:

1) Augmentation Pipeline Optimization:
Current results suggest blanket augmentation application degrades overall performance, necessitating smarter augmentation strategies. Potential approaches include:

a) Adversarial augmentation: Using reinforcement learning to develop mission-specific augmentation policies

b) Sensor fusion augmentation: Correlating visual degradations with IR/radar sensor characteristics

c) Dynamic scheduling: Gradually introducing harsh augmentations as training progresses

The 6.8% recall improvement under fog conditions demonstrates augmentation value for specific operational environments. Developing weather-prediction-coupled augmentation systems could enable anticipatory model tuning based on mission forecasts. Furthermore, combining geometric transformations (rotation, scaling) with photometric augmentations may better simulate sensor movement in mobile platforms.

2) Multi-Modal Integration Opportunities:
Future systems could enhance visual identification through:

a) RF signature correlation: Matching visual detections with electronic warfare sensor data

b) Acoustic profiling: Cross-validating vehicle engine signatures

c) Contextual awareness: Integrating geographic and mission data for likelihood estimation

The study's visual-only approach achieves militarily useful accuracy (84.6%) but remains below the 95% threshold required for autonomous engagement decisions. Hybrid systems combining visual classification with IFF transponders and battlefield management system inputs could bridge this gap while maintaining redundancy.

C. Closing statement

This comprehensive analysis demonstrates both the potential and limitations of current AI-driven object detection systems in military situational awareness applications. The YOLOv8 architecture, particularly in its s-variant configuration, proves capable of friend-foe identification tasks when leveraging pre-trained weights and strategic augmentation policies. Key implementation insights include the superiority of transfer learning over from-scratch training, optimal model size selection relative to dataset scale, and context-dependent augmentation efficacy.

ACKNOWLEDGMENT

This work was supported by the NSP SD program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. D01-74/19.05.2022.

REFERENCES

[1] Yibo Sun and Zhe Sun and Weitong Chen, The evolution of object detection methods https://www.sciencedirect.com/science/article/pii/S095219762400616X, 2024.

[2] Iliev, R., A. Genchev. Possibilities for using unmanned aerial vehicles to obtain sensory information for environmental analysis Information & Security: An International Journal 46, no. 2 : 127-140. https://doi.org/10.11610/isij.4609, 2021

[3] Iliev, R., A. Genchev. Generalized net model of the decision making process in the crisis management Journal 'Advanced Studies in Contemporary Mathematics', 31 No 4 pp 401 - 409, http://dx.doi.org/10.17777/ascm2021.31.4.401, 2021

[4] Iliev R., Kochankov M. A generalized net model of command and control system, Vol. 2 Environment. Technology. Resources. Proceedings of the 15th International Scientific and Practical Conference. Volume 2 / Information Technologies, pp. 127 - 131, https://doi.org/10.17770/etr2024vol2.8035, 2024.

[5] Munir, Arslan, Alexander Aved, and Erik Blasch, Situational Awareness: Techniques, Challenges, and Prospects https://doi.org/10.3390/ai3010005, 2022.

[6] Joint Publication 3-09, Joint Fire Support https://web.archive.org/web/20140411125036/http://www.dtic.mil/doctrine/new pubs/jp3 09.pdf, 2010.

[7] Joseph Redmon, Ali Farhadi, YOLOv3: An Incremental Improvement https://pjreddie.com/media/files/papers/YOLOv3.pdf, 2018.

[8] Glenn Jocher and Ayush Chaurasia and Jing Qiu, Ultralytics YOLOv8 https://github.com/ultralytics/ultralytics, 2023.

Buslaev, Alexander, Vladimir I. Iglovikov, Eugene Khvedchenya, Alex Parinov, Mikhail Druzhinin, and Alexandr A. Kalinin, Albumentations: Fast and Flexible Image Augmentations https://doi.org/10.3390/info11020125, 2020.

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 209-212

A Model for Using Drones for Medical Reconnaissance in Combat Operation

Nikolay Nichev
Georgi Benkovski, Bulgarian Air Force Akademy
Dolna Mitropolia, Bulgaria
Nicheff@gmail.com

Krasimir Koynakov
Logistics and Tehnology department, Vasil Levski National Military University
Veliko Turnovo, Bulgaria
Krasi.koynakov@gmail.com

***Abstract*— This paper presents a model for the use of unmanned aerial vehicles in the medical support of military formations at the tactical level. The medical support system of the Armed Forces of the Republic of Bulgaria is described and a model for the use of drones by the medical posts of military formations in combat operations is presented, emphasizing the use in the field of medical intelligence, deployed elements and minimum technical requirements for unmanned aerial vehicles to ensure the implementation of medical support tasks.**

Keywords — drone, medical intelligence, military formations, evacuation, support.

I. INTRODUCTION

Medical support is a complex of activities carried out with the aim of strengthening, protecting and restoring the health of personnel in peacetime, during operations in crises, conflicts and during war. Medical support is an element of the National Health System and is organized in accordance with the Geneva and Hague Conventions. The main goal is to ensure the prevention of injuries and diseases, timely and adequate medical care and evacuation, specialized treatment and rehabilitation, by maintaining reliable, secured and flexible medical capabilities, complementary or supplementing those in the collective defense system. [1]

A. Medical support of military formations

Military medical facilities (MMFs) are organizational structures in which doctors and dentists, independently or with the help of other medical and non-medical specialists, carry out activities related to the medical support of the Armed Forces. MMFs are divided into four groups, levels, called "Roles" according to the capabilities they possess, increasing on a progressive basis, to conduct treatment, evacuation, supply with medical equipment and other activities that are essential for maintaining the health of the personnel of the military formations. "Roles" are defined in accordance with the available minimum clinical capabilities, and not capacity and maneuverability. The minimum capabilities of each MMF are generally included in the capabilities of the higher level, so that Role 3 can perform the functions of Role 1 and Role 2. A MMF cannot have lower capabilities than those assigned to it. Therefore, it cannot have a Role (X) – minus. [2]

The scope of medical support activities is defined as "Roles" from 1 to 4, corresponding to the standards adopted in NATO in the logistics doctrine.

Role 1. It is carried out in formations up to the battalion/regiment level under the leadership of a doctor and includes the provision of the following types of medical care:

- emergency medical care,
- primary outpatient medical and dental care,
- stabilization and preparation of patients for evacuation,
- medical evacuation of sick, injured and those in need of specialized care,
- preventive military medicine, including health promotion and a complex of hygienic, prophylactic and anti-epidemic measures.

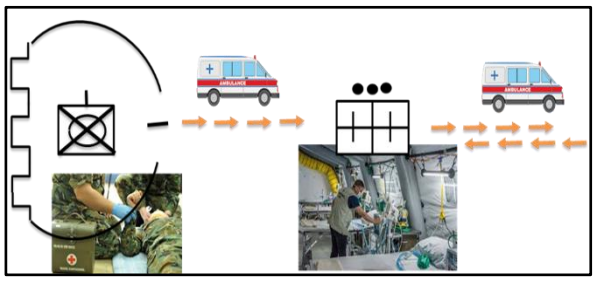


Fig. 1. Role 1

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8509
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

Role 2. Usually carried out at the brigade level, serving also adjacent formations. It includes:

- evacuation from Role 1, reception and triage of patients,
- stabilization of vital signs and treatment of shock,
- control of injuries, provision of life-saving surgical care and treatment of lightly injured and sick until their return to the formation,
- preparation of patients for further evacuation, with the possibility of temporarily taking patients (until they are stabilized) in a situation of mass casualties or interruption of the evacuation chain,
- activities in preventive medicine, dentistry, stress management and strengthening of mental health.

Role 2 is classified as "Role 2 - basic" and "Role 2 - reinforced". The individual units in both types of Role 2 are built on a modular principle, with the possibility of reinforcing Role 1 if necessary.

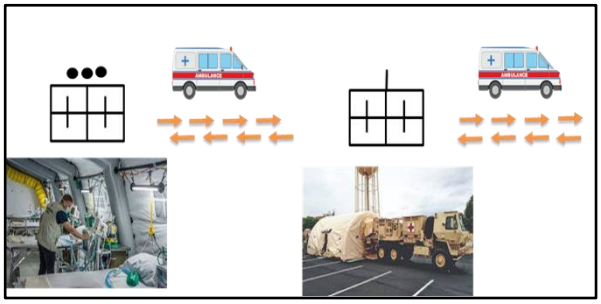


Fig. 2. Role 2

Role 3. It is carried out in medical institutions for hospital care (field or stationary) and includes:

- reception of patients from Role 2 or directly from the site of the injury/incident,
- triage of victims for evacuation to Role 4 or hospitalization of wounded and sick, who can be provided with comprehensive assistance and ensure return to the line, in accordance with the evacuation policy,
- provision of specialized medical care by specialist doctors, without which patients would not withstand evacuation to the institutions at the next level.

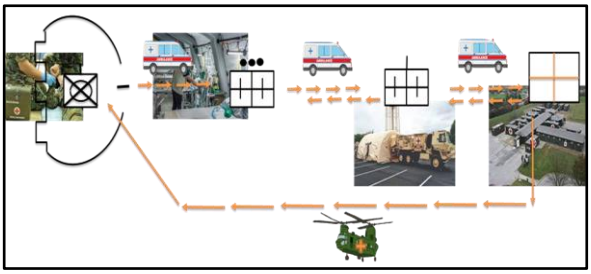


Fig. 3. Role 3

Role 4. It is carried out in medical institutions with the highest level of competence and includes:

- reception of patients from Role 3, other medical points directly from the site of injury/incident,
- provision of comprehensive medical care, reconstructive surgery and rehabilitation of patients until their final recovery. [3]

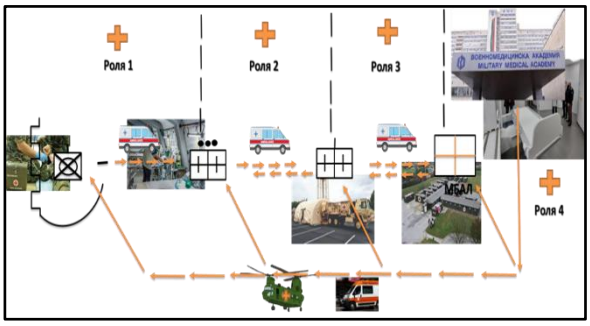


Fig. 4. Role 4

Medical forces and assets maintain the same level of readiness, mobility and protection as the forces provided. Medical care is provided adequately, continuously and progressively, ranging from first aid to comprehensive specialized care and rehabilitation. The means of evacuating victims must allow for continuity of care during transportation. Medical activities in wartime operations, as well as in crises, are as close as possible to the standard of medical care in peacetime. Medical care is provided in the shortest possible time: first aid within 10 minutes; medical care within 1 hour and surgical care within 2 hours. Achieving the "golden hour" for providing surgical care implies the most favorable outcome of the treatment of the victim. The wounded and sick are sorted into categories, depending on the urgency of treatment, the need and the method of evacuation [3].

Medical intelligence (MI) is a type of intelligence (activity) whose product is intelligence information obtained from medical, bioscientific, epidemiological and environment-specific information, as well as other information affecting human health and lives. This information also includes an assessment of the medical capabilities of the military and civilian sectors of potential hostile parties (opposing forces) or other entities in the area of intelligence responsibility/interest. The specificity of this intelligence information, which is of a specific nature, requires the necessary medical expertise during both stages of the intelligence cycle - planning and processing.

Medical intelligence as a subgroup of intelligence works within the same framework and uses the intelligence cycle to ensure that all available information is processed to make assessments. Medical intelligence as phenomenon should be totally coordinated with the planning of the operations of the tactical and operational level of national armed forces in national operations and as a joint effort in NATO. The cycle must be synchronized with the decision-making process, troop leading procedures and operational requirements of the commander in order to successfully influence the outcome of the operation. [4] The MEDINT (medical intelligence) cycle provides a process for understanding and sequencing the activities involved in MEDINT products and is useful as an aid to understanding the

interrelationships that exist between the different phases. The MEDINT process may not continue throughout the entire cycle and there are no hard boundaries delineating the points at which each stage of the cycle begins and ends. [5]

The stages or steps in the medical intelligence cycle are:

- Direction,
- Collection,
- Processing,
- Dissemination.

Medical evacuation (ME) is part of medical support and includes transportation, supportive treatment, medical control and care for medical casualties from the place of their occurrence to military medical (civilian) medical facilities or between them. Medical evacuation, depending on the means used, is ground, air and sea. It is carried out in three phases: forward (from the place of injury to the first point of treatment within the area of operation), tactical (within the TO) and strategic (outside the TO).The means of NME are ambulances and ambulance buses equipped to provide medical care. There are also tracked medical evacuation vehicles, as well as wheeled armored personnel carriers (APCs) for medical evacuation. Some of the most famous medical variants of infantry fighting vehicles (IFVs) nowadays are: AMX, AMX-10, Bradley, BVP M 80-A, KIFV, Kurganets-25, MLVM, MT-LB, Tulpar. Similarly, the most common APCs, used for medical purposes are: AIFV, Bandvagn-206, Boragh, Bulldog, FV-432, Stormer, Wiesel. [6]

From the other hand, ambulances are the most common type of ground transport vehicle for medical evacuation. There are variations in their capacity and capabilities. For evacuation from the front end, protected ambulances with limited (for supporting basic vital functions) capacity for providing medical care are used. For evacuation between medical facilities, ambulances (resuscitation vehicles) equipped with high-tech medical equipment and trained personnel are used. Primary MEDEVAC provides transport of patients from the site of injury to the initial place of providing assistance to the injured. This is required by operational circumstances in order to meet clinical deadlines and is therefore increasingly carried out by rotational teams in the front areas. MEDEVAC referrals can be to medical facilities of any role and should be made whenever possible to the most appropriate level of care within the time frame, not necessarily to the nearest medical facility. Primary MEDEVAC should be configured to meet similar levels of force protection as the forces in the area they are required to enter. Similarly, since primary MEDEVAC may provide evacuation of casualties prior to initial resuscitation, primary MEDEVAC teams should be equipped and trained to provide appropriate pre-hospital care. [7]

II. MATERIALS AND METHODS

The current model was developed based on experiments conducted at the Vasil Levski Military University during complex tactical exercises using a drone. During the exercises, medical reconnaissance tasks were performed, such as searching for wounded on the battlefield and directing transport vehicles to the assembly points for the wounded and supporting ground medical evacuation. The analysis conducted at the end of the complex tactical exercises is the basis for developing a model for the use of unmanned aerial vehicles by the medical posts of military formations.

The essence of the experiment is as follows.

The experiment was carried out using a DJI Mavic Pro 2 unmanned aerial vehicle, and tasks related to the logistical support of a mechanized battalion in field conditions were planned and executed. After completing the tasks, an analysis was made for the performance such as time, data transmission, difficulty of performance. During the execution of the tasks, the information from the UAV is transmitted to live data in a deployed logistic support control center (LSCC). The UAV is managed by a specialist operator from the control center, and the received data is recorded and processed by officials in the composition of the LSCC.

III. RESULTS AND DISCUSSION

For the use of drones in the medical support of military formations, it is necessary to open departments at medical posts. The personnel of the departments will consist of three drone operators, who will work from a deployed post in the area of the medical post under the direct control of the head of the medical post. They must be trained in the operation and maintenance of unmanned aerial vehicles.

Unmanned aerial vehicles must have the following minimum technical characteristics:

- Speed (near sea level, no wind) 72 kph (S-mode),
- Takeoff Altitude 6000 m,
- Flight Time (no wind) 31 minutes (at a consistent 25 kph),
- Hovering Time (no wind) 29 minutes,
- Flight Distance (no wind) 18 km (at a consistent 50 kph),
- Wind Speed Resistance 29–38 kph,
- Pitch Angle 35° (S-mode, with remote controller) 25° (P-mode),
- Angular Velocity 200°/s,
- Operating Temperature Range-10°C to 40°C,
- Operating Frequency 2.400 - 2.483 GHz 5.725 - 5.850 GHz,
- GNSS GPS+GLONASS,
- Hovering Accuracy Range

Vertical:

± 0.1 m (when vision positioning is active)
± 0.5 m (with GPS positioning)

Horizontal:

± 0.3 m (when vision positioning is active)
± 1.5 m (with GPS positioning),

- Internal Storage 8 GB.

In the model described above, the medical point will have the following elements:

- sorting post - it is where examinations of the injured are carried out and the levels of medical care are determined. If medical interventions can be performed within the MB, they are accepted for treatment. Otherwise, they are stabilized and prepared for subsequent evacuation,
- places for receiving and accommodating injured people,
- isolator - a place for treating infectious patients,
- places for resting the personnel of the BMP,
- a place for those waiting for subsequent evacuation,
- a workplace for a psychologist - activities are carried out to prevent combat stress and work with those who have suffered combat stress,
- a site for partial sanitary treatment,
- drone post - a place for drone operators to work.

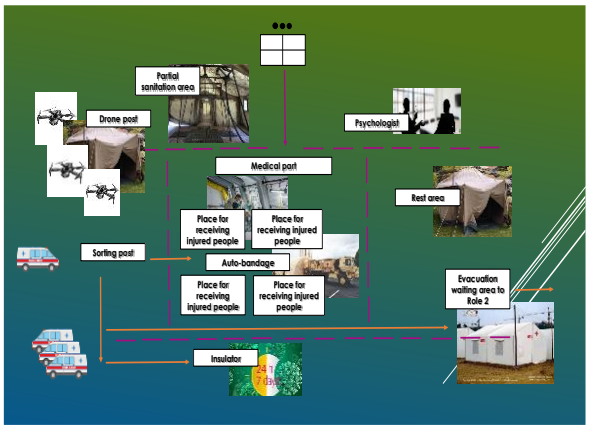


Fig. 5. Medical center

Main tasks of the deployed drone post:

1. Conducting medical reconnaissance, which includes:
   - searching for wounded on the battlefield,
   - reconnaissance of routes for evacuating wounded with medical transports,
   - monitoring and directing vehicles carrying medical supplies and materials,

2. Directing medical transport vehicles to the nests for collecting the wounded.

3. Processing and analyzing data received from unmanned aerial vehicles.

Necessary material resources to ensure the uninterrupted operation of the drone post:

- drones – 4 pcs. – 3 for performing medical support tasks and 1 in reserve,
- spare propellers for the drones – 2 sets,
- power batteries – 12 pcs. (x 3 per drone),
- laptops – 3 pcs. (for each operator),
- radio means for communication with the drivers of the sanitary transport vehicles.

IV. CONCLUSIONS

The use of unmanned aerial vehicles in the medical support of military formations greatly increases their capabilities, especially when performing medical reconnaissance tasks. The described model needs to be applied when conducting complex tactical exercises.

V. ACKNOWLEDGMENTS

This report is in implementation of the National Scientific Program "Security and Defence", adopted by Decree of the Council of Ministers No. 731 of 21.10.2021.

REFERENCES

[1] Doctrine of the Armed Forces of the Republic of Bulgaria NP-1, National publication, Sofia, 2017. [Doktrina na Vyoryjenite sili na Republika Bulgariq – NP-1, Nacionalna publikaciq, Sofiq, 2017].

[2] Medical Support Doctrine - NP-4.10, National publication, Sofia, 2020. [Doktrina za medicinsko osigurqvane - NP-4.10, Nacionalna publikaciq, Sofiq, 2020].

[3] Logistics Doctrine NP-4. National publication, Sofia, 2019. [Doktrina za logistikata NP-4, Nacionalna publikaciq, Sofiq, 2019].

[4] N. Pavlovski, Planning of Combat Actions by the Company and Platoon according to the Formation Management Procedures (Troop Leading Procedures). Veliko Tarnovo: Vasil Levski National Military University, 2024, pp. 13, 14, 15. [Planirane na boĭnite deĭstviya ot rotata i vzvoda sŭglasno protsedurite za upravlenie na formirovaniyata (Troop Leading Procedures). Veliko Tŭrnovo: Natsionalen voenen universitet Vasil Levski, 2024, s. 13, 14, 15]. (ISBN 978-954-753-390-5 – soft cover, ISBN 978-954-753-391-2 – pdf and ISBN 978-954-753-392-9 – CD).

[5] Allied joint medical doctrine for medical intelligence AJMedP-3, Edition A Version 2, Published by the Nato Standardization Office (NSO), August, 2020.

[6] N. Pavlovski, Handbook of Combat Armored Tracked Vehicles. Veliko Tarnovo: Vasil Levski National Military University, 2025, pp. 24, 26, 40, 42, 52, 62, 66, 68, 86, 96, 100, 102, 114, 118, 120. [*Narŭchnik za boĭni bronirani verizhni mashini.* Veliko Tŭrnovo: Natsionalen voenen universitet Vasil Levski, 2025, s. 24, 26, 40, 42, 52, 62, 66, 68, 86, 96, 100, 102, 114, 118, 120]. (ISBN 978-954-753-408-7 – softcover, ISBN 978-954-753-409-4 – pdf and ISBN 978-954-753-410-0 – CD).

[7] Allied joint medical doctrine for medical evacuation - AJMedP-2, Edition A Version 1, Published by the Nato Standardization Office (NSO), August, 2018.

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 213-217

Analysis of a Radiological Incident in Nuclear Power Plant and Simulation of the Radioactive Material Dispersion

Nikolay Iliyanov Padarev
„V. Levski" NMU
Faculty of Security and Defence
Veliko Tarnovo, Bulgaria
nipadarev@gmail.com

Nikolay Todorov Dolchinkov
„V. Levski" NMU
Faculty of Security and Defence
Veliko Tarnovo, Bulgaria
n_dolchinkov@abv.bg

***Abstract*— The report examines the behaviour of a radionuclide released during an accident at a nuclear power plant. The analysis focuses exclusively on caesium to provide specific and detailed information about its characteristics and dispersion. Experiments were conducted under different atmospheric stability conditions to track changes in the plume's behaviour.**

The hypothetical model used in this analysis can be easily applied to assess radiation scenarios in similar events. This approach is instrumental in assisting first responders and guiding defensive actions. It also aids in establishing general operational guidelines and evaluating population exposure risks.

Keywords*— *radiological event, hazard, modelling and simulation, atmospheric dispersion, radionuclide, cesium-137, NPP accidents.

I. INTRODUCTION

The security of nations is increasingly threatened by asymmetric threats, including those posed by national and international terrorism. According to international humanitarian law (IHL), the deliberate use of radiological hazards as weapons could be considered a violation of the principles of distinction and proportionality, key elements in the protection of civilian populations during armed conflict. Radiological weapons or incidents that cause indiscriminate harm may also violate the prohibition against causing unnecessary suffering, as outlined in the Geneva Conventions and their Additional Protocols. Such weapons can exploit vulnerabilities in populations, creating psychological distress, inflicting life-threatening harm, and causing long-term environmental damage, all of which are contrary to the fundamental protections afforded under IHL. Furthermore, certain radioactive particles, such as alpha emitters, pose detection challenges, requiring specialized personnel and equipment for mitigation, which may not be readily available, further complicating humanitarian responses and recovery efforts in accordance with IHL obligations. [1]-[4]

Depending on the characteristics of radiological agents, they can affect personnel, equipment, and infrastructure through neutron or gamma irradiation, as well as contamination by alpha or beta particles. Radiation exposure occurs through direct irradiation, external contamination (contact with skin and clothing), or internal contamination (inhalation or ingestion). [5]

Radiological leakage encompasses accidental releases, indirect damage, or deliberate sabotage targeting nuclear, industrial, or medical facilities that handle radioactive materials. [6]-[8] These facilities include, but are not limited to, nuclear power plants, research reactors, nuclear fuel processing and enrichment plants, radioactive waste storage facilities, and medical or industrial sites that utilize radioactive sources.

Additionally, radiological hazards can arise from transportation accidents involving radioactive materials transported via road, rail, or water. Ensuring protection against NPP accidents is a matter of national security, as such incidents have direct consequences for both human safety and environmental integrity. The primary objective of this research is to demonstrate the use of software tools for simulating radiological dispersion following an NPP accident. The simulation assists in determining potential evacuation routes, identifying affected areas, and predicting radioactive fallout. Given the prevalence of radioactive elements in nu-clear energy production, it is crucial to develop decision-support systems that minimize risks to the population and environment.

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8468
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

Radiation accidents typically involve significant emissions within the first 10–12 days. Most major fission products, including isotopes of tellurium (Te), iodine (I), barium (Ba), lanthanum (La), cerium (Ce), ruthenium (Ru), strontium (Sr), yttrium (Y), zirconium (Zr), niobium (Nb), silver (Ag), and cesium (Cs), can be detected in atmospheric aerosols from the radioactive cloud. Fortunately, alpha-emitting nuclides tend to remain near the accident site in limited quantities. [9]

II. MATERIALS AND METHODS

Protection against radiation exposure requires strict adherence to absorbed dose limits for workers and the general population. Annual total body equivalent dose limits are set at 1 mSv for the public and 50 mSv for occupational workers.

To simulate the dispersion of ^{137}Cs, a specialized software tool was employed to model various atmospheric conditions. Radioactive materials released during NPP accidents disperse in the form of gases and particles, with their concentration in air and deposition on soil dependent on several factors, including:

1) Amount of radionuclide released.
2) Height of the emission source.
3) Wind speed and atmospheric stability.

Physical and chemical properties of the released material.

The Hotspot software suite was used to simulate emergency response scenarios, assess facility safety, and estimate the dispersion of radioactive plumes. Hotspot's atmospheric dispersion model provides a first-order approximation of radiological effects associated with short-term (less than 24 hours) releases, primarily applicable to near-surface emissions in open terrain under various weather conditions.

The simulation incorporated two scenarios: 1) A release of ^{137}Cs accompanied by fire and 2) A release of ^{137}Cs accompanied by an explosion.

Cesium-137 was chosen due to its significant role in radiation exposure following nuclear incidents, such as the Chernobyl disaster. The primary objective was to evaluate its dissipation within the first hour of the incident. [10]

Hotspot utilizes the Gaussian plume model, which has been extensively validated for initial dispersion estimates and worst-case safety analyses. The software integrates radiation dosimetry methodologies recommended by the International Commission on Radiological Protection (ICRP) and Environmental Protection Agency (EPA) guidelines.

The mathematical model used to estimate airborne radioactive concentration (C) at a given location is expressed as follows [11]:

$$C(x,y,z,H) = \frac{Q}{2\pi\sigma_y\sigma_z u} exp\left[-\frac{1}{2}\left(\frac{y}{\sigma_y}\right)^2\right]$$
$$\left\{exp\left[-\frac{1}{2}\left(\frac{z-H}{\sigma_z}\right)^2\right]\right\}$$
$$++exp\left[-\frac{1}{2}\left(\frac{z+H}{\sigma_z}\right)^2\right] exp\left[-\frac{\lambda x}{u}\right].DF(x) \quad (1)$$

Where:

C - time-integrated atmospheric concentration (Ci-s/m³);

Q - source term (Ci);

H - effective release height (m);

X -radioactive decay constant (s^{-1});

u - wind speed at release height (m/s);

σ_y, σ_z - standard deviations in lateral and vertical plume spread (m);

DF(x) - depletion factor accounting for deposition losses.

Since the release can be of longer or shorter duration, this parameter can be modified by introducing a dispersion correction factor $\sigma_y^{'}$ [11-13]:

$$\sigma_y^{'} = \sigma_y \left(\frac{t}{10}\right)^2 \quad (2)$$

The following values were selected for baseline data: material at risk (MAR) $1{,}5.10^{16}$ Bq, damage ratio (DR) 1,00, leakage factor 1,00, air fraction (ARF) 1,00, a respirable fraction (RF) of 1,00 and a deposition rate of 0,15 cm/s. Specifically, in the case of the accompanying fire, the cloud height is set to 10 m. For the general explosion scenario, all parameters were unchanged, adding an explosive with 90,9 kg (200 lb) of TNT. [14]

The maximum deposition rate can reach up to 6. 10^{-2} $m.s^{-1}$ in some cases. However, the rate of deposition depends on atmospheric stability. Under moderately stable atmospheric conditions (usually at night, clear skies), Jensen [15] proved that u is only half of its value under neutral conditions. Thus, the maximum deposition rate should then, according to equation (3), be only a quarter of the value, i.e. < 1,5. 10^{-2} $m.s^{-1}$.

$$v_i = \frac{u_*^2}{u} \quad (3)$$

The deposition rate includes two components: v_i eddy diffusion and v_s sedimentation. This is an important expression that puts an upper bound on the eddy–diffusion component of the total deposition rate. u_* is proportional to the frictional tangential rotation speed of the particles in the flow.

Boundary conditions were selected in terms of total equivalent dose equivalent TEDE and land deposition (soil radioactivity value in kBq/m^2). For TEDE, the intrinsic, mean, and extrinsic parameters were defined as 5 Sv

(25 rem) (threshold for immediate deterministic effects), 20 mSv (0,2 rem) (maximum dose for first responders), and 1 mSv (0,1 rem) (evacuation operational level). Values of 3700 kBq/m^2 (100 µCi/m^2), 370 kBq/m^2 (10 µCi/m^2) and 37 kBq/m^2 (1 µCi/m^2) were selected for the internal, medium and external terrestrial deposition parameters. The total effective dose equivalent (TEDE), which includes external and internal contributions to the total absorbed dose and deposition of the contaminant on the ground, has been calculated for different categories of atmospheric stability, several particle size distributions of the contaminant, different amount of explosive.

The meteorological conditions under which the research was done are wind speed at a height on 10 m is 10 m/s, for the stability of the atmosphere very stable vertical resistance A and neutral D on the Pasquil–Gifford scale was used.

Simulation models offer risk-free testing, cost savings, and efficiency improvements across various fields. They enhance decision-making by analysing different scenarios, support hands-on training, and accelerate innovation. Their predictive power helps forecast trends, optimize operations, and improve scalability. Overall, simulations provide a flexible and effective way to experiment, learn, and plan. [16]-[20]

III. RESULT AND DISCUSSION

The HotSpot software allows the user to visualize both TEDE contour plots and radioactive deposition contour plots, which show the relative values as a function of distance along the plume line. Radioactive deposition contour plots for the scenario are shown in Fig. 1 (a, b).

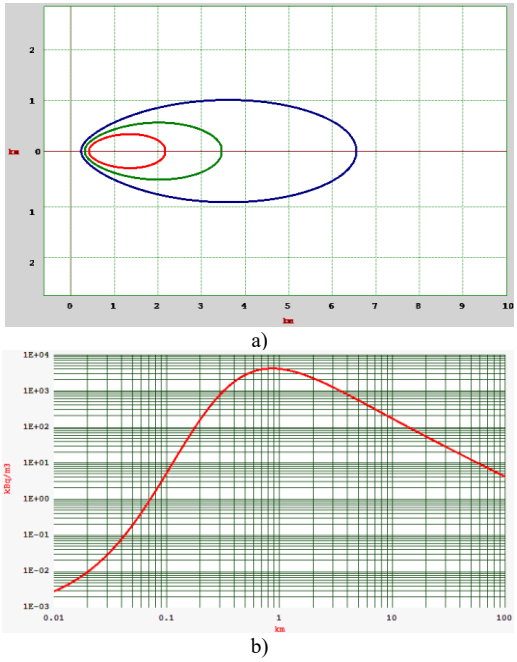


Fig. 1. Dependence of terrestrial radioactive deposition on the center of the accident accompanied by fire in vertical stability class A: a) areas of radioactive deposition b) graphical dependence on concentration and distance

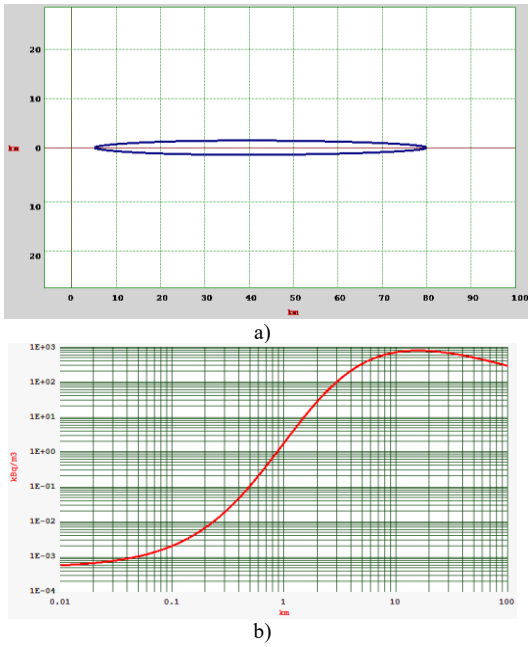


Fig. 2. Dependence of terrestrial radioactive deposition on the center of the accident accompanied by fire in vertical stability class A: a) areas of radioactive deposition b) graphical dependence on concentration and distance

Figures 1 and 2 depict the results of the simulation of a radiation accident and the dispersal of ^{137}Cs. In the input data presented above, for vertical resistance class A, the zones have clearly defined boundaries, with personnel at approximately 2 km from the accident site potentially absorbing up to 5 Sv. The red zone covers an area of 0,92 km^2. The zone where no values exceeding 1 mSv (0,1 rem) are observed is considered the operational evacuation threshold and is 10,7 times larger than the red zone.

The measured Total Effective Dose Equivalent (TEDE) values indicate that the selected conditions do not pose a deterministic risk, as the corresponding threshold (5 Sv) is not reached. For vertical resistance class D, a terrestrial radiation deposition zone of up to 37 kBq/m^2 (1 µCi/m^2) extends up to 80 km from the accident site.

In the simulation of a radiation accident with an accompanying explosion under the specified conditions, the probability of fatality reaches up to 99 % for individuals located within 10 m of the accident site. The TEDE values again indicate that the selected conditions do not lead to a deterministic risk, as the 5 Sv threshold is not exceeded. However, the simulation revealed areas with TEDE values exceeding 20 mSv, extending up to 0,5 km for vertical resistance A and 1 km for vertical resistance D, necessitating the immediate evacuation of the area.

Furthermore, considering the outer affected area, which ranges from 9,5 km² to 286 km², it can be inferred that at a maximum distance of approximately 95 km from the accident site, under vertical resistance class D, radiative deposition at the Earth's surface would reach at least 1 mSv.

Contour plots for terrestrial deposition illustrate the maximum distances with depositional boundaries from the centre of dispersal (hot spot). Comparing the areas obtained for resistance class A, the outer zone extends 9,8 km² in the case of fire and 9,5 km² in the case of an explosion, showing insignificant differences. However, the blue zone areas measure 168 km² and 286 km², respectively, demonstrating that the resistance class significantly impacts the spread of ^{137}Cs following a nuclear power plant accident involving an explosion, unlike scenarios with fire alone.

This experimental evidence further confirms that the Hotspot software platform can reliably simulate the release of ^{137}Cs in a nuclear power plant accident of this magnitude.

IV. CONCLUSIONS

Hotspot allows users to create a custom "mixture of radionuclides." However, for the purposes of this development, we have chosen to estimate the release of a single radionuclide to better understand its contribution to the Total Effective Dose Equivalent (TEDE). The software enables the visualization of both ground deposition and TEDE contours at the release site in Google Earth by incorporating the geographic coordinates of the reactor where the incident occurred.

Managing the risk of a radiological event is crucial, as it cannot be eliminated, regardless of how robust the nuclear power plant (NPP) protection system is. Atmospheric dispersion modelling software plays a vital role in mitigating the impact of radiological dispersion during such events. Due to the limited availability of specific contamination data following NPP accidents, certain parameter approximations were necessary to construct comparative scenarios. However, the deposition scenario can be replicated with comparable magnitudes under different initial conditions, such as variations in elevation and wind speed.

For this scenario, the General Explosion and General Fire models within the Hotspot code have proven to be effective in estimating the ground deposition of ^{137}Cs.

The author contributed to the adaptation and customization of the Hotspot modelling environment for the purposes of scenario analysis, specifically focusing on the release and deposition patterns of cesium-137. The comparative modelling methodology developed by the author allows for quick scenario reconstruction with limited data, making it applicable in both civil protection planning and training of emergency response teams.

The obtained results can be used for:

- Preparing emergency response strategies for potential radiological incidents.
- Developing training simulations for CBRN (Chemical, Biological, Radiological, Nuclear) protection units.
- Supporting national risk assessments and crisis management protocols involving NPPs.
- Enhancing public safety by contributing to evacuation planning and contamination zone prediction.

These contributions not only support scientific understanding of atmospheric radionuclide dispersion but also provide a practical toolset for decision-makers and first responders.

V. ACKNOWLEDGEMENTS

This research is supported National Science Program „Security and Defense", adopted with RMS No. 731 of 21.10.2021 and according to Agreement No. D01-74/19.05.2022.

REFERENCES

[1] Н. Недев, „Условия за приложимост на международното хуманитарно право в контекста на съвременните военни операции," Научна конференция „Знание, наука, иновации, технологии", 26–27 септември 2024 г., Велико Търново, ISSN 2815-3472 (Print), ISSN 2815-3480 (CD), pp. 775–783.

[2] Н. Недев, „Същност и съдържание на международноправна уредба за защита на правата на човека в условията на въоръжен конфликт," Научна конференция „Знание, наука, иновации, технологии", 26–27 септември 2024 г., Велико Търново, ISSN 2815-3472 (Print), ISSN 2815-3480 (CD), pp. 784–794.

[3] Н. Недев, „Специфика на международното хуманитарно право в условията на съвременните въоръжени конфликти," Научна конференция „Знание, наука, иновации, технологии", 13 декември 2024 г., Велико Търново, ISSN 2815-3480 (CD), pp. 1455–1468.

[4] Н. Недев, „Предизвикателства пред международното хуманитарно право при водене на бойни действия в градски условия," Научна конференция „Знание, наука, иновации, технологии", 13 декември 2024 г., Велико Търново, ISSN 2815-3480 (CD), pp. 1469–1485.

[5] N. Dolchinkov and N. Nichev, "Gamma-background radiation control systems as a factor of Bulgaria's national security," Environment. Technology. Resources., Proc. 15th Int. Sci. and Pract. Conf., vol. IV, Rezekne, Latvia, 2024, pp. 83–88. https://doi.org/10.17770/etr2024vol4.8225.

[6] R. Marinov, "Model of management of processes and phenomena's in the military security system," Environment. Technology. Resources., Proc. 15th Int. Sci. and Pract. Conf., vol. IV, Rezekne: Rezekne Academy of Technologies, 2024, pp. 173–177. https://doi.org/10.17770/etr2024vol4.8188.

[7] R. Marinov, "Contemporary challenges to the protection of the country's sovereignty," Environment. Technology. Resources., Proc. 15th Int. Sci. and Pract. Conf., vol. IV, Rezekne: Rezekne Academy of Technologies, 2024, pp. 168–172. https://doi.org/10.17770/etr2024vol4.8187.

[8] Б. Димитров, „Методи за *регистриране и наблюдение на йонизиращи лъчения," в* Сб. доклади от научна конференция „Актуални проблеми на сигурността", том 4, НВУ „Васил Левски", 2017, стр. 140–147.

[9] A. Andrew, G. S. George, and S. Haupt, "Utilizing state estimation to determine the source location for a contaminant," Atmospheric Environment, vol. 46, pp. 580–589, 2012.

[10] J. Peterson, M. MacDonell, L. Haroun, and F. Monette, Radiological and Chemical Fact Sheets to Support Health Risk Analyses for Contaminated Areas, USA, 2007.

[11] H. Shin and J. Kim, "Development of realistic RDD scenarios and their radiological consequence analyses," 2009, pp. 1516–1520.
[12] V. A. Sharifi, M. Rahimi-Movaghar, Mohammadi, *et al.*, "Analysis of mental health research in the Islamic Republic of Iran over 3 decades: A scientometric study," East Mediterr. Health J., vol. 14, pp. 1060–1069, 2008.
[13] Н. Николов, „Прибори и системи за мониторинг, откриване, идентифициране, предупреждение и отчитане на химични, биологични и радиоактивни агенти,“ в Годишна университетска научна конференция, том 5, НВУ „В. Левски“, 2019, с. 73–80.
[14] N. O. Jensen, "A Micrometeorological Perspective on Deposition," Health Phys., vol. 40, 1981.
[15] N. Tonchev, V. Gaydarov, and N. Hristov, Analyzes and applications through the computational approach DEFMOT, Sofia, 2022, pp. 167.
[16] H. Pantsar, *et al.*, "Effect of Processing Parameters on the Microstructure and Hardness of Laser Transformation Hardened Tool Steel," Proc. 23rd Int. Congress on Applications of Laser and ElectroOptics (ICALEO*)*, San Francisco, CA, USA, 2004, pp. 565–573.
[17] N. Dolchinkov, L. Lazov, J. Ivanov, D. Nedyalkov, and L. Linkov, "Study of cutting and labeling of polymethylmethacrylate using a CO2 laser," *Environment. Technology. Resources.*, Proc. 12th Int. Sci. and Pract. Conf., vol. 3, 2019, pp. 37–40. https://doi.org/10.17770/etr2019vol3.4203.
[18] N. Tontchev and E. Yankov, "Multi-criteria support for decision-making by shifting restrictions," *Int. Sci. Conf.* Mathematical Modeling, no. 1, 2017.
[19] I. Minevski, *Risk in the transportation of dangerous goods by land transport*, Monograph, Publishing National University of the Republic of Bulgaria, V.T., 2018, pp. 17.
[20] E. Yankov and T. Gueorguiev, "A critical overview of the normative, regulatory and international standard requirements for healthy and safe public facilities," 2022 8th Int. Conf. on Energy Efficiency and Agricultural Engineering (EE&AE), Ruse, Bulgaria, 2022, pp. 1–4. doi: 10.1109/EEAE53789.2022.9831293.

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 219-223

Adjusting the Quantity of Surfactants in Decontamination Solutions

Nikolay Iliyanov Padarev
„V. Levski" National Military University
Faculty of Security and Defence
Veliko Tarnovo, Bulgaria
nipadarev@gmail.com

***Abstract*— A comparative analysis of non-ionic, anionic, and cationic surfactants was conducted to evaluate their potential use in the decontamination of radioactive contamination. The study produced both graphical and analytical representations of the relationship between surfactant concentration and surface tension. These findings enable precise control over the selection and concentration of surfactants in decontamination solutions, optimizing their effectiveness for specific application.**

***Keywords*— CBRN decontamination, surface tension, surfactant, effectiveness, Wolfram Mathematica, radioactive contamination.**

I. Introduction

The limited capabilities for providing adequate and timely protection to the population and infrastructure necessitate improving the effectiveness of mitigating the consequences of chemical, radiological, and biological events. [1]-[10] The relevance of this report arises from the increased requirements for the characteristics of solutions used in specialized decontamination processes, emphasizing both the thoroughness of the decontamination and environmental protection. Surfactants are a critical component of decontamination solutions for radiological, chemical, and biological agents, enhancing their wetting properties. It is therefore advisable to explore alternatives to the currently used compositions that contain surfactants. Studies on the surface tension of special treatment solutions are particularly relevant, as surface tension directly affects their performance characteristics [11, 12].

The lack of qualitative and quantitative characterization of the performance properties of surfactants and detergents in decontamination formulations, which could potentially replace synthetic base products, represents a significant scientific challenge addressed in this report.

The report presents studies on the surface tension of various formulations containing surfactants, aiming to achieve optimal wetting properties in decontamination solutions. Selecting the appropriate surfactant requires consideration of various factors. From the studies conducted, it can be concluded that surfactants must be carefully chosen for each specific application. To streamline the selection process, surfactants can be compared to identify a few that are more effective than others. Typically, surfactants are used in combination with other surfactants and decontaminating agents. These combinations aid in removing a wide range of radiological, chemical, and biological contaminants.

Surfactants are a vital component of decontamination solutions as they enhance wetting properties. One of the primary requirements for decontamination solutions is the effective removal of pollutants from contaminated surfaces. Adding a surfactant to water decreases the surface tension of the solution and improves its wetting ability. [13]

Aqueous surfactant solutions are used to decontaminate radioactive contamination. In the Bulgarian Army, the decontamination composition DV-2 is in use, which contains alkylphenol polyglycol ethers, sodium tripolyphosphate, and sodium sulphate. This study aimed to conduct a comparative analysis of the wetting capabilities of water solutions containing DV-2 and alternative surfactant-based solutions under varying temperature and concentration conditions.

The purpose of this report is to develop a methodology for qualitative and quantitative assessment on the wetting action of solutions to eliminate radiological, chemical and biological agents.

Objects of the research are water solutions DV-2 (Alkylphenolpolyglycol Ethers, Sodium three Polyphosphate and Sodium Sulphate), water solutions on Diethanolamide of Coconut Oil Acids ($C_{(7+n)}H_{(15+2n)}NO_3$, n

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8469
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

= 5, 7, 9, 11, 13, 15), n-Alkyl Dimethyl Benzyl Ammonium Chloride ($C_9H_{13}NClR$, where R = C_{12} H_{25}, C_{14} H_{29} or C_{16} H_{33}), Sodium Lauryl ether Sulphate ($C_{12}H_{25}O.(C_2H_4O)2.SO_3.Na$).

II. Materials and Methods

The report describes an experimental setup using the "Maximum Pressure When Blowing a Bubble from the Capillary" method, which is widely applied in practice. This method has been modified by incorporating a tempering coil to regulate the solution's temperature. A schematic representation of the setup is shown in Fig. 1.

The essence of the method lies in determining the maximum pressure (p_max) required to blow a bubble from the end of the capillary. A schematic diagram of the apparatus used for measuring surface tension is presented in Fig. 1. The dimensions of Rebinder's vessel are as follows: height – 10 cm, diameter – 12 cm.

The key component of Rebinder's vessel is the capillary (4)—a pipette graduated from 0.1 cm³, with an inner radius of 0.00043 m. The capillary is positioned inside the vessel (1) so that its end is immersed 5 mm into the liquid being tested. When a vacuum is created in the system, an air bubble will emerge from the capillary once the external pressure becomes sufficient to overcome the surface tension of the liquid. [14, 15]

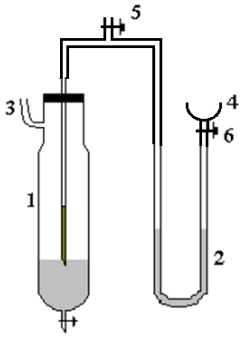


Fig. 1. Schematic of an experimental set-up for determining the surface tension by the "Maximum pressure when blowing a bubble from the capillary" method.

1) Rebinder's vessel, 2) water pressure gauge 3) hole for charging the system with the solution under study; 4) pressure vessel; 5) and 6) taps.

Before starting the measurements, the tightness of the vessel is checked. To do this, tap (7) is closed, and tap (5) is opened.

The capillary constant is determined as follows: Vessel (1) is washed several times and then filled up to the mark. Tap (5) is opened, allowing water to be drawn through tube (3) from the side hole, after which the tube is sealed with a plug. Then, tap (6) is opened, and by removing the pressure vessel (4), the water level in both legs of the manometer is adjusted to zero on the scale. After closing tap (6), the manometer tube is raised again until the water level aligns with the uppermost divisions on the manometer scale. At this point, tap (5) is closed.

By slowly and carefully opening tap (6), the water in the pressure vessel flows into the pressure gauge, creating a difference in liquid levels between the two legs of the manometer. As a result, the liquid in the manometer shifts to the left leg. Now when an air bubble separates from the capillary, the difference in liquid levels between the two legs of the manometer is recorded as h_0.

The surface tension of water (σ_0) at the corresponding temperature is taken from a reference book. After determining the capillary constant, the differences in liquid levels between the two legs of the manometer for the tested liquids (h) are measured. When the maximum difference in levels is reached, a bubble is blown, causing the difference to decrease. However, for calculations, the maximum difference is required, not the difference after the bubble is blown.

For the purposes of the dissertation experiment, the working temperatures of the solutions were controlled by cooling to 10°C and heating with a heater, with the liquid passing through a tempering tube in vessel (1). [15]

When blowing a bubble from the capillary, the surface tension (σ) and maximum pressure (P_{max}) required to detach the bubble from the capillary are related by the following equation:

$$\sigma = \frac{r}{2}(p_{max} - hpg) \quad (1)$$

where:

- r – radius of the capillary (m)
- h – depth of capillary immersion (m)
- g – gravitational acceleration (9.80665 m/s² at sea level)
- ρ – liquid density (kg/m³)
- σ – surface tension (N/m)

Equation (1) is expressed in terms of quantities that can be directly measured. The maximum pressure (P_{max}) is determined using a water manometer. Since accurately measuring the capillary radius (r) can be challenging, this measurement can be bypassed if the experiment is conducted with a liquid of known surface tension (e.g., distilled water):

$$\sigma_0 = \frac{r_0}{2}(P_{0max} - h\rho_0 g) \quad (2)$$

where the index "0" indicates the values that apply to water. By eliminating r_0 from (1.) and (2.), the dependence is obtained:

$$\sigma = \sigma_0 \frac{P_{max} - h\rho g}{P_{0max} - h\rho_0 g} \quad (3)$$

To calculate the maximum pressure required to blow a bubble out of the capillary (3) one can write:

$$\sigma = \sigma_0 \frac{H - h}{H_0 - h} \quad (4)$$

Where:

- H – difference in water manometer levels for the investigated solution (m)
- H_0 – difference in water manometer levels for distilled water (dH_2O) (m)
- h – capillary immersion depth (m)
- σ – surface tension (N/m)

One advantage of this method is that surface tension is determined at a moment when the contact angle is zero. This eliminates the need to account for the θ-parameter, whose determination is often associated with significant error.

The method is dynamic and should be conducted as slowly as possible to ensure an accurate determination of P_{max}. To minimize errors, it is recommended to perform the experiment at least five times. If variations occur in the measurements, the reported differences should be averaged to improve reliability. We used Wolfram Mathematica to create the mathematical models. Wolfram Mathematica is a powerful computational software system used across various fields such as mathematics, science, engineering, and data analysis. It combines symbolic and numerical computation, data visualization, and the creation of interactive interfaces all in one platform.

The software allows for algebraic manipulations like simplifying expressions, differentiation, and solving equations symbolically. It also supports numerical computations with high precision, optimization, and numerical integration. Mathematica offers strong data analysis capabilities, including statistics and machine learning. For visualization, it can generate both 2D and 3D graphics of high quality.

Wolfram Language is the programming language of Mathematica, enabling the development of functions, scripts, and interactive applications. This makes it extremely useful in academia, research, and various industrial sectors. [16]-[18]

III. RESULT AND DISCUSSION

The research was conducted over a concentration range using three types of surfactants, each in different concentration intervals due to their varying rates of surface tension reduction.

Figures 2, 3, and 4 present charts illustrating the correlation between surface tension (σ) and concentration (c) as σ = f(c). Figure 5 shows a chart of DV-2.

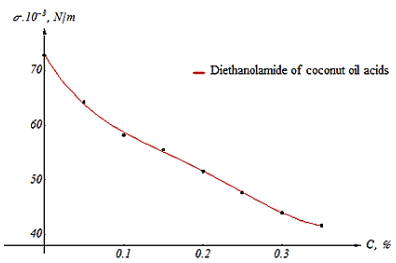


Fig. 2. Surface Tension versus Concentration of Diethanolamide of Coconut Oil Acids.

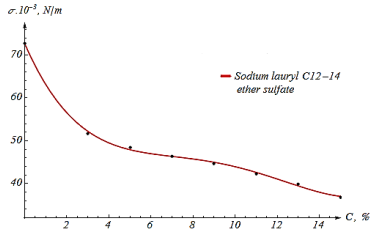


Fig. 3. Surface Tension versus Concentration of Sodium Lauryl Ether Sulphate.

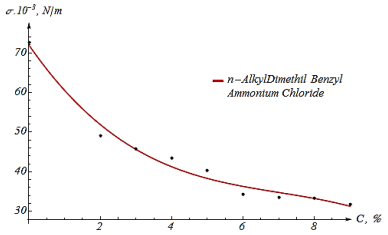


Fig. 4. Surface Tension versus Concentration of n-Alkyl Dimethyl Benzyl Ammonium Chloride.

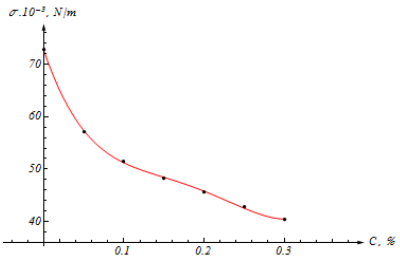


Fig. 5. Surface Tension versus Concentration of DV-2.

If DV-2 is used within a concentration range of 0.1% to 0.2%, it may be replaced with Diethanolamide of Coconut Oil Acids at a concentration of no less than 0.28%.

The other surfactants shown in Figures 2 and 4 exhibit a decrease in surface tension over higher concentration intervals. Therefore, if Sodium Lauryl Ether Sulfate or n-Alkyl Dimethyl Benzyl Ammonium Chloride is used, a larger amount must be added to the decontamination solution.

Analytically, the interdependence between surface tension and concentration can be described using regression equations, formulated with the Wolfram Mathematica software [11, 12, 13]. Statistically processed correlation data for DV-2 and Diethanolamide of Coconut Oil Acids, along with their regression equations at 20°C, are presented in equation (5).

$$\sigma = a[0] + a[1].C + a[2].C^2 + a[3].C^3 + a[4].C^4 \quad (5)$$

where:

σ - surface tension [N/m],

C- concentration [%],

a – coefficients.

TABLE 1. STATISTICAL EVALUATION OF EXPERIMENTAL DATA ON DV-2.

	Estimate	Standard Error	t-Statistic	P-Value
a[0]	72.6875	0.385222	188.69	0.0000280856
a[1]	−449.783	21.8892	−20.5482	0.00236001
a[2]	3457.58	337.974	10.2303	0.00942006
a[3]	−12775.8	1762.44	−7.24891	0.0185041
a[4]	16848.5	2916.26	5.77744	0.0286767

TABLE 2. STATISTICAL EVALUATION OF EXPERIMENTAL DATA FOR DIETHANOLAMIDE DERIVED FROM COCONUT OIL FATTY ACIDS.

	Estimate	Standard Error	t-Statistic	P-Value
a[0]	72.8218	0.407361	178.765	3.85991×10^{-7}
a[1]	−238.533	19.0153	−12.5442	0.00109218
a[2]	1402.4	246.499	5.68926	0.0107645
a[3]	−4933.11	1095.24	−4.50413	0.02044
a[4]	6129.09	1552.61	3.94761	0.0289901

Diethanolamide of Coconut Oil Acids offers numerous benefits, making it a preferred choice for radioactive decontamination solutions. It belongs to the group of non-ionic surfactants, which play a crucial role in surface tension reduction and improving wetting properties.

One of the key characteristics of non-ionic surfactants is their ability to adsorb onto a negatively charged water/air interface, effectively reducing the surface load and film thickness. This process creates conditions for electrostatic destabilization, which can enhance contaminant removal. However, due to this property, non-ionic surfactants often require combination with ionic surfactants to achieve better control over surface charge and film stability. This synergy between non-ionic and ionic surfactants ensures optimal detergency and wetting efficiency in decontamination solutions.

IV. CONCLUSIONS

Various substances and formulations can be used in radioactive decontamination solutions to lower surface tension, provided they undergo a preliminary quantitative and qualitative assessment of their wetting ability. The empirical correlations established between surface tension and concentration can be effectively applied after statistical processing of experimental data. These correlations are crucial for optimizing the efficacy and performance of decontamination solutions.

It is recommended to use aqueous solutions of Diethanolamide of Coconut Oil Acids in the concentration range of 0.2% to 0.3%, as they exhibit wetting properties like DV-2 at a concentration of 0.1% to 0.2%.

Additionally, the Wolfram software can be utilized to generate graphical and analytical dependencies for various surfactants, allowing for a more precise evaluation of their surface tension behaviour and effectiveness in decontamination applications.

V. ACKNOWLEDGEMENTS

This research is supported National Science Program „Security and Defense", adopted with RMS No. 731 of 21.10.2021 and according to Agreement No. D01-74/19.05.2022.

VI. DISCLOSURE OF INTERESTS

The author has no competing interests.

REFERENCES

[1] N. Dolchinkov, "Construction of a system for monitoring the pollution of water bodies with waste," Environment. Technology. Resources., Rezekne, Latvia, Proc. 15th Int. Sci. Pract. Conf., vol. I, pp. 136–141, 2024. [Online]. Available: https://doi.org/10.17770/etr2024vol1.7989

[2] N. Dolchinkov and N. Nichev, "Gamma-background radiation control systems as a factor of Bulgaria's national security," Environment. Technology. Resources., Rezekne, Latvia, Proc. 15th Int. Sci. Pract. Conf., vol. IV, pp. 83–88, 2024. [Online]. Available: https://doi.org/10.17770/etr2024vol4.8225

[3] R. Marinov, "Model of management of processes and phenomena's in the military security system," Environment. Technology. Resources., Proc. 15th Int. Sci. Pract. Conf., vol. IV, pp. 173–177, 2024. [Online]. Available: https://doi.org/10.17770/etr2024vol4.8188

[4] R. Marinov, "Contemporary challenges to the protection of the country's sovereignty," Environment. Technology. Resources., Proc. 15th Int. Sci. Pract. Conf., vol. IV, p. 168, 2024. [Online]. Available: https://doi.org/10.17770/etr2024vol4.8187

[5] Б. Димитров, „Методи за регистриране и наблюдение на йонизиращи лъчения," в Сб. доклади от научна конференция „Актуални проблеми на сигурността", том 4, НВУ „Васил Левски", 2017, стр. 140–147.

[6] E. Yankov and T. Gueorguiev, "A critical overview of the normative, regulatory and international standard requirements for healthy and safe public facilities," 2022 8th Int. Conf. on Energy Efficiency and Agricultural Engineering (EE&AE), Ruse, Bulgaria, 2022, pp. 1–4. doi: 10.1109/EEAE53789.2022.9831293.

[7] N. Dolchinkov, L. Lazov, J. Ivanov, D. Nedyalkov, and L. Linkov, "Study of cutting and labeling of polymethylmethacrylate using a CO2 laser," 12th Int. Sci. Pract. Conf. Environment. Technology. Resources., vol. 3, pp. 37–40, 2019. [Online]. Available: https://doi.org/10.17770/etr2019vol3.4203

[8] N. Tontchev and E. Yankov, "Multi-criteria support for decision-making by shifting restrictions," Int. Sci. Conf. Mathematical Modeling, no. 1, 2017. DOI: 10.13140/RG.2

[9] I. Minevski, Risk in the Transportation of Dangerous Goods by Land Transport. V.T.: Publishing House of the National University of the Republic of Bulgaria, 2018, p. 17.

[10] N. Dolchinkov, N. Nichev, and Y. Boyanova, "Uranium mines in Bulgaria - Analysis of the state 30 years after their closure," Environment. Technology. Resources., Rezekne, Latvia, Proc. 15th Int. Sci. Pract. Conf., vol. I, pp. 123–129, 2024. [Online]. Available: https://doi.org/10.17770/etr2024vol1.8002

[11] N. I. Padarev, "Selection on nonionic surfactants in the decontamination solution," Int. J. Knowledge, Skopje: Inst. of Knowledge Management, 2016, pp. 451–455.

[12] N. I. Padarev, P. Peneva, and D. Tsvetkov, "Surface activity of solutions for eliminating radioactive contamination," Machines, Technologies, Materials, no. 5, pp. 48–50, 2015.

[13] P. Peneva and N. Padarev, "Surface activity of solutions for eliminating radioactive contamination," Machines, Technologies, Materials, no. 4, pp. 10–13, 2014.

[14] Z. M. Zorin, V. D. Sobolev, and N. V. Churaev, "Changes in capillary pressure, surface tension, and viscosity of liquids in quartz microcapillaries," Coll. Rep. IV Conf. on Surface Forces, Nauka, Moscow, 1972.

[15] P. Peneva, Laboratory Manual for Physical Chemistry Exercises, NVU, VT, 1994.

[16] S. Wolfram, The Mathematica Book, Champaign, IL: Wolfram Media, 1999.

[17] Wolfram, "Mathematica Official Website." [Online]. Available: www.wolfram.com/mathematica/. [Accessed: Sept. 12, 2024].

[18] B. B. Lee, P. Ravindra, and E. S. Chan, "New drop weight analysis for surface tension determination of liquids," Colloids and Surfaces A: Physicochem. Eng. Aspects, 2009, pp. 112–120.

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 225-236

Migration as a Hybrid Threat: Legal Perspectives on Countering Illegal Migration and the Lithuania-Belarus Border Crisis

Aurelija Pūraitė
Mykolas Romeris University
Kaunas, Lithuania
aurelija.puraite@mruni.eu

Danguolė Seniutienė
Mykolas Romeris University
Kaunas, Lithuania
desniutiene@mruni.eu

***Abstract*- Migration has increasingly been weaponized as a tool of hybrid warfare, challenging national security, legal frameworks, and humanitarian obligations. This article examines migration as a hybrid threat through a legal lens, focusing on recent trends in countering illegal migration and the implications of the Lithuania-Belarus border crisis. The article explores the strategic use of migration by state and non-state actors to destabilize target countries, assessing how hybrid threats manifest in border crises. It provides a legal analysis of state responses, including legislative measures, border control policies, and international legal obligations concerning asylum and human rights. The case study of the Lithuania- Belarus border crisis illustrates how irregular migration can be leveraged as a form of coercion, examining the legal justifications and challenges of Lithuania's response, including pushbacks, emergency measures, and EU legal frameworks. Furthermore, the article discusses recent trends in countering illegal migration, highlighting developments in EU law, technological advancements in border management, and cooperative mechanisms among states. It evaluates the legal and ethical dimensions of restrictive measures, considering their compliance with international human rights law, the principle of non-refoulement, and European legal standards. By analyzing legal frameworks and state responses, the article aims to contribute to the broader discourse on security, migration law, and hybrid threats. It underscores the need for a balanced approach that upholds national security while adhering to international legal norms. The findings emphasize the necessity of legal adaptability in addressing evolving hybrid threats, ensuring that countermeasures remain both effective and lawful.**

Keywords*- *hybrid threats, illegal migration, Lithuania-Belarus border, migration crisis, national security.

I. Introduction

In recent years, the dynamics of migration have been increasingly influenced by state actors seeking to manipulate refugee flows for political or strategic gain. One of the most notable instances of this phenomenon has been the migration crisis along the Lithuania-Belarus border. In 2021, Lithuania, alongside other Baltic states, faced an unprecedented surge in illegal border crossings, a situation which the Lithuanian government and the European Union (EU) attribute to deliberate actions by the Belarusian regime. On July 29, 2021, during a session of the Permanent Council of the Organisation for Security and Cooperation in Europe (OSCE), Lithuania vehemently rejected Belarus's claims of mistreating migrants and pointed out that the refugee flows were being artificially engineered by Belarus as a means of exerting political pressure. Lithuanian representatives underscored that Belarus's actions, which involved facilitating the movement of migrants towards the EU, were part of a broader strategy aimed at destabilizing Lithuania and its EU allies [1].

This situation can be framed as a hybrid threat, where migration is used not only as a tool of destabilization but also as a means of manipulating political outcomes. Hybrid threats, by their very nature, involve a blend of conventional and unconventional methods to achieve strategic objectives, often blurring the lines between what is considered an act of war and what is seen as a non-military challenge. In this case, Belarus's orchestrated migration crisis is both an attempt to undermine the EU's cohesion and a retaliatory response to European sanctions

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8506
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

and Lithuania's support for Belarusian opposition figures [2]. This weaponization of migration has led to significant challenges for Lithuania, both in terms of its internal security and its international relations, as the influx of undocumented migrants from Belarus continues to strain border control measures and generate widespread political tension.

The European Union, in turn, has assisted Lithuania and other affected states, yet the crisis continues to evolve, raising critical legal and security concerns. Lithuania's recent amendments to the Law on the Legal Status of Foreign Persons [3], aimed at enhancing border security and managing the crisis, have been met with controversy. While Lithuania defends these legal changes as necessary to ensure the protection of its borders, human rights organizations have raised concerns over the legality of these actions in light of international refugee law [1]. This tension between national security measures and adherence to international legal obligations presents a complex challenge in understanding how best to counteract such hybrid threats while maintaining the integrity of human rights and international law.

In this article, we will explore the legal dimensions of Lithuania's response to the Belarusian-driven migration crisis, examining the ways in which illegal migration has been utilized as a tool of hybrid warfare and the legal implications for the European Union. By analyzing the situation from a legal perspective, this article aims to highlight the delicate balance between ensuring national security and fulfilling international obligations to protect refugees and asylum seekers.

II. Materials and Methods

This article employs a qualitative research approach, utilising document analysis and case study methodology to examine the Lithuania-Belarus border crisis in the context of hybrid threats. The study relies on academic literature, policy documents, and reports from international organisations to assess the security implications of hybrid migration tactics. A comparative analysis of EU migration policies and national security strategies was conducted to highlight policy gaps and the evolving nature of irregular migration as a geopolitical tool. The research also incorporates expert opinions and secondary sources to provide a multidimensional perspective on the crisis. Furthermore, a critical review of legislative frameworks and institutional responses was performed to evaluate the effectiveness of existing measures. This methodological approach ensures a comprehensive and structured examination of the topic while integrating theoretical insights with practical policy considerations.

III. Results and Discussion

A. Theoretical analysis of hybrid threats: orchestrated illegal migration

The manifestations of hybrid threats may be seen in the news, and institutions like NATO and EU prepare policy documents on the concept, but the concept is not easy to define. The Council of Europe report notes that "there is no universally agreed definition of "hybrid war" and there is no "law of hybrid war". [4]. The term "hybrid threats" appears more and more often in nowadays international political discussions and other fields. Other terms used are "hybrid warfare", "hybrid conflicts", "hybrid tactics", "hybrid confrontations", "hybrid operations", etc. [5]. All these, in essence involve the orchestrated use of a wide range of instruments to coerce an opponent. Such instruments involve cyber-attacks, economic blackmail, information warfare, exploitation of ethnic divisions [6]; mass disinformation campaigns, including fake news, in particular via social media, disruption of communications and other networks and many others. Sanz-Caballero notes that "non-exhaustive list of hybrid threats would also include cyberattacks, terrorism, organised crime, drug trafficking, migration flows, economic or financial wars, media exploitation, and the application of covert psychological operations. The most updated catalogues of hybrid threats intertwine multiple political, economic, technical, social, informational, legal, diplomatic, scientific, and military risks [7]. The Council of Europe (2016) further notes that "it is commonly agreed that the main feature of this phenomenon is 'legal asymmetry', as hybrid adversaries, as a rule, deny their responsibility for hybrid operations and try to escape the legal consequences of their actions. Different academic sources [8-11] collectively underscore the complexity and multifaceted nature of hybrid threats, highlighting their reliance on ambiguity, non-linear tactics, and the exploitation of various domains to achieve strategic objectives. Hybrid threats represent an evolution in the understanding of modern warfare, merging conventional military strategies with irregular tactics and cyber operations. The security literature highlights the complexity and ambiguity inherent in hybrid threats. These threats are designed to operate in the "grey zone" between peace and war, making it difficult for states to identify and respond effectively.

However, despite their presence in a grey area, hybrid adversaries are not exempt from legal rules. Overall, international law, with a specific emphasis on international human rights law, remains relevant. Additionally, it is crucial to acknowledge that addressing hybrid threats falls under the jurisdiction and obligation of individual states [7]. When it comes to holding states accountable for hybrid actions, the main difficulty lies in the attribution of

responsibility. States often use proxies to carry out activities in the grey zone. However, simply claiming that a hybrid threat originated within a state's territory is not enough to hold that state responsible. To attribute a specific act, carried out by an individual or group, to a particular state, several stringent conditions must be met. These conditions typically involve complex elements that are challenging to prove. As a result, operations within the grey zone provide significant advantages to those using such tactics.

The term "hybrid warfare" is now intimately linked to Russia. The term itself was coined in 2002 by William J. Nemeth to describe the Chechen insurgency that blended (hence the word 'hybrid') traditional societal organisation and guerrilla warfare with modern military tactics and use of technology– from mobile telephones to the internet [12]. Russia's strategic documents (for example, [13-14]) indicate that the country has expanded beyond traditional hybrid warfare tactics -such as conventional, irregular, terrorist, and criminal methods - by incorporating a wide range of strategies, including information, cyber, economic, diplomatic, political, and social tactics. In close cooperation with Belarus, Russia leverages these hybrid approaches, with illegal immigration being one of the key tools employed to destabilize neighboring countries. By fostering instability and uncertainty, Russia aims to undermine the governance and resilience of its adversaries, making them more vulnerable to Russian influence and control. Hybrid tactics are used by Russia to safeguard its strategic interests, including maintaining access to warm-water ports, securing energy transit routes, and ensuring favorable political regimes in nearby states. Consequently, scholars like Mark Galeotti [15], Michael Kofman, and Matt Rojansky [16] have argued that Russia's methods now enter an area that is not fully understood or defined by both scholars and defense experts. Multiple scholars and security analysts (including Pomerantsev and Weiss [17]; Fridman [18]; Nilsson [19]; Watling, Danylyuk & Reynolds [20]; Mumford & Carlucci [21]; Pynnöniemi & Jokela [22]) identify three key characteristics that distinguish Russia's hybrid warfare, which has been furthered by Belarus as a proxy.

First, there is a "kinetic" component involving the deployment of armed forces and occasional combat engagements. However, Russian troops often operate with more autonomy and precision than traditionally expected. Beyond the "military war," there is a significant "intelligence war" dimension. The Kremlin has heavily invested in its intelligence community, including the Foreign Intelligence Service (SVR), the Main Intelligence Directorate (GRU), and the Federal Security Service (FSB), which increasingly participates in overseas operations. These agencies are not only focused on intelligence gathering but also serve as tools for non-linear warfare, spreading disinformation, encouraging defections, and disrupting or corrupting command and communication channels. In recent years, Belarus has become an active partner in this strategy, particularly in weaponizing illegal migration. Belarus has facilitated the flow of migrants into the European Union as a form of political retaliation, acting as a proxy for Russia to create instability and exert pressure on EU countries, especially Lithuania and Poland.

A third focal point of the Kremlin's hybrid warfare is the "information war," which aims to promote Russia's narrative while undermining those of its adversaries. This includes efforts to win the battle for hearts and minds, such as through the RT international television station, which not only promotes the Kremlin's perspective but also challenges Western media orthodoxy with a blend of genuine investigative journalism, disinformation, and conspiracy theories. This combination of kinetic, intelligence, and information warfare, along with Belarus's involvement in facilitating illegal migration, reflects a broader strategy to destabilize the region and weaken the EU's political cohesion.

The use of illegal migration as a hybrid threat has been increasingly evident at the Lithuania- Belarus border, with Belarus playing a central role in facilitating the movement of migrants across the European Union's eastern frontier. As part of its broader strategy to destabilize neighboring countries and exert political pressure on the European Union (EU), Belarus has been accused of deliberately orchestrating and encouraging the illegal flow of migrants, particularly from the Middle East, towards the EU border. This strategy is widely seen as part of a broader geopolitical confrontation with Lithuania, Poland, and the EU, following tensions related to the political situation in Belarus.

The Belarusian regime, under President Alexander Lukashenko, has been actively facilitating the transport of migrants from conflict zones such as Afghanistan, Iraq, and Syria, offering them easy access to Belarusian territory with the aim of pushing them across the EU's borders into Lithuania and Poland. This manipulation of migration flows is not just a border control issue but a strategic maneuver designed to create instability, undermine EU unity, and shift the political dynamics in Belarus's favor. As noted by Surwillo & Slakaityte [23], this strategy effectively weaponizes migration, turning it into a tool for Belarus to counter EU sanctions and pressure.

In 2021, the number of illegal crossings from Belarus into Lithuania surged dramatically. As the crisis deepened,

Lithuania, supported by EU agencies, strengthened its border defenses and implemented stricter immigration policies. However, Belarus continued to encourage the movement of migrants, even offering transport, in what could be seen as an effort to exploit vulnerabilities within the EU's asylum system. As Russia's closest ally, Belarus acted as a proxy in Moscow's attempt to destabilize the EU and its member states [24]. The use of illegal migration as a hybrid weapon has become one of the tools in this complex strategy, which also includes cyberattacks, disinformation, and political manipulation.

The ongoing border crisis illustrates how hybrid threats have evolved to include non-traditional tactics, where the manipulation of migration flows becomes a means of coercion and political leverage. This not only challenges traditional border security measures but also tests the resilience of European governance structures. Moreover, it calls into question the EU's ability to respond effectively to such asymmetric threats, especially when they are coordinated by state actors like Belarus, with tacit support from Russia.

B. Legal environment related to migration crisis and operational challenges

Lithuania's response to hybrid threats also sparked discussions on the need to reassess existing legal and institutional frameworks. The crisis exposed the limitations of current migration governance models and underscored the necessity for a cohesive EU response that incorporates both legal and operational aspects of migration management. This involves not only safeguarding the integrity of external borders but also ensuring adherence to international obligations concerning refugee protection.

The border crisis between Lithuania and Belarus highlights how migration management and hybrid threats intersect, demanding a comprehensive approach that surpasses traditional legal structures. As states contend with the increasingly sophisticated strategies of adversarial actors, adaptive legal and operational responses become essential. The lessons learned from Lithuania's experience are crucial for shaping future policies at both national and EU levels, enhancing the ability to address the complexities of hybrid threats in migration management.

In recent years, the legal frameworks surrounding migration management have been scrutinized in light of the increasing irregular migration exacerbated by hybrid threats. The Lithuania-Belarus border crisis serves as a key case study, demonstrating the challenges faced by states in navigating international law while trying to uphold sovereignty and ensure national security [25].

International law, particularly through customary treaties and practices, serves as the foundation for protecting the rights of migrants and refugees. Instruments like the 1951 Refugee Convention and its 1967 Protocol [26], alongside various human rights treaties, obligate states to refrain from deporting refugees or asylum seekers to countries where they may face persecution. However, the rise of hybrid threats, including the use of migration as a geopolitical weapon, complicates adherence to these principles. Lithuania's situation is further complicated by Belarus's approach to migration, which involves exploiting vulnerable populations to destabilize the EU's borders.

Although Lithuania is bound by EU regulations governing asylum management, including the Schengen Code and the Common European Asylum System (CEAS), it was forced to adopt extraordinary measures in response to the surge of migrants encouraged by the Belarusian authorities. Measures such as the declaration of a state of emergency and the construction of border barriers raised significant legal concerns regarding their compatibility with international obligations. While these actions can be justified on national security grounds, they risk violating migrants' rights, particularly in terms of access to asylum procedures and the right to international protection. This creates a tension between national security and the protection of human rights.

Moreover, the operation of international law reveals intrinsic limits in scenarios involving hybrid threats. The principle of non-refoulement, essential for migrant protection, requires a careful balance between legal obligations, which may not always align with national interests. The Lithuania-Belarus crisis exemplifies this discrepancy. Lithuania's proactive measures, including border operations, enhanced surveillance, and swift deportation processes, often clash with the obligations of international humanitarian law and EU asylum standards. As a result, these countermeasures can create tensions between safeguarding national integrity and upholding the rights of individuals in transit.

The evolving landscape of international law faces challenges in its interpretation and application when confronted with hybrid threats. The inadequacies in the legal frameworks governing migration management, particularly those responding to external pressures, highlight the need for a reconceptualization of how international law can adapt to the dynamic nature of hybrid threats. Lithuania's experience demonstrates that while international law offers valuable tools for managing

migration, the legal certainty it provides can be obscured in times of crisis.

In summary, the legal frameworks surrounding irregular migration within the context of hybrid threats reveal intricate and often conflicting relationships between international law and national security strategies. Lithuania's increasingly militarized approach to migration management underscores the urgent need for global legal reforms that effectively address modern challenges while adhering to fundamental human rights principles (as in [25]). The quest for a balanced response to irregular migration in complex geopolitical contexts remains a fundamental challenge for states as they navigate the tension between border control imperatives and their international law responsibilities.

In response to the growing influx of migrants at the Lithuania-Belarus border during the 2021 crisis, the Lithuanian government adopted several national legal measures to manage this unprecedented situation. These included both existing laws and rapid legislative reforms, reflecting a reactive policy response to the hybrid threats exacerbated by illegal migration and broader geopolitical tensions. A key issue in evaluating these national laws is their compatibility with the legal norms and obligations of the EU.

One significant legislative measure taken by Lithuania was the declaration of a state of emergency in August 2021 [27], which facilitated expedited asylum claims processing and migrant detention management. This state of emergency, which was extended several times, allowed Lithuania to implement enhanced border control measures and establish temporary accommodation sites for migrants. However, such actions raised substantial legal concerns regarding their alignment with the EU's CEAS, particularly regarding asylum seekers' rights and the principle of non-refoulement, which prohibits returning individuals to countries where they face harm.

To address the specific challenges of the crisis, Lithuania amended its law on the legal status of foreigners in July 2021 (as mentioned in [3]). These changes allowed the arrest of migrants crossing the border illegally and set stringent criteria for granting asylum. Critics, including human rights organizations, argued that these amendments could undermine the legal protections for asylum seekers under EU law, potentially restricting access to effective asylum procedures.

Lithuania also utilized provisions within EU directives, particularly the Asylum Procedures Directive (2013/32/EU) [28], which permits member states to implement accelerated procedures when faced with large numbers of asylum applications. However, such provisions must still respect fundamental EU rights and principles, an issue that was contentious during the border crisis. Reports indicated instances where migrants experienced prolonged detention and inadequate access to legal assistance, raising doubts about Lithuania's compliance with EU standards.

Lithuania also relied on international support and cooperation with neighboring countries, including active participation in joint operations with Frontex, the European Border and Coast Guard Agency, to strengthen border security through increased surveillance and resource allocation. However, the shifting dynamics of EU responsibility-sharing in response to hybrid threats introduced tensions between member states. Concerns were raised over Lithuania's bilateral agreements with Belarus, particularly since these agreements must align with international standards regarding the treatment of refugees and migrants.

To institutionalize its approach to border management, Lithuania established a migration management framework that integrated the efforts of multiple agencies, combining law enforcement and social services. This framework aimed not only to curb illegal migration but also to address the socio-economic needs of incoming migrants. These legal and institutional adaptations were scrutinized for their effectiveness and consistency with broader EU frameworks.

As the situation at the Lithuania-Belarus border evolved, the interplay between national legislation and EU legal standards highlighted the complexities of balancing an immediate crisis response with established human rights norms. Ongoing legal challenges and public debates regarding Lithuania's adherence to EU obligations demonstrate the need for a balanced approach to migration management, particularly in environments marked by hybrid threats.

One of the primary operational challenges was the allocation of limited resources in the face of a surge in irregular migration. Lithuanian authorities had to mobilize substantial financial and human resources to manage this influx. However, the limited budget resources created significant pressure on national policies and capabilities, which were already strained due to COVID-19-related budgetary restrictions. This lack of financing made it difficult to respond to the crisis effectively and hindered the development of long-term strategies that could integrate legal structures with operational capabilities.

Additionally, Lithuania faced the challenge of enhancing border surveillance amid its legal obligations

under international law and EU regulations on external border management. Monitoring the vast and often challenging terrain along the Lithuania-Belarus border posed significant logistical difficulties. To counter the hybrid threats posed by Belarus, which included not only manipulating migration flows but also conducting disinformation campaigns and psychological operations aimed at destabilizing Lithuania's governance, Lithuania invested in technological resources to strengthen border surveillance. This included the use of drones, infrared cameras, and additional border patrol personnel, all of which required rapid implementation despite bureaucratic and legal obstacles related to procurement and deployment.

Furthermore, the deployment of security forces on the border raised significant questions regarding compliance with human rights standards and the treatment of migrants. Lithuania's migration policies during this period were subject to intense scrutiny, both domestically and internationally, particularly in terms of balancing national security imperatives with the obligation to protect the dignity and rights of migrants and asylum seekers. The operational challenge of ensuring adherence to international standards was exacerbated by reports of violations of EU law and the Refugee Convention. As a result, Lithuania had to navigate complex legal frameworks concerning human rights and asylum while pursuing its national interests in border security.

Coordinating efforts across various sectors also proved challenging during the crisis. A comprehensive migration management response required collaboration between the Ministry of the Interior, the State Border Guard Service, police agencies, and humanitarian organizations. However, differing priorities among these entities often hindered effective cooperation and resulted in inconsistencies in policy implementation. The lack of a coherent interagency strategy complicated operational responses to both the urgent humanitarian needs of migrants and the broader national security concerns.

In conclusion, the operational challenges Lithuania faced during the crisis at its Belarus border highlight the tensions inherent in migration management frameworks. The interplay between resource allocation, border surveillance strategies, legal compliance, and interagency coordination reveals the complexities of implementing effective migration policies in the face of hybrid threats. Recognizing these operational challenges is essential for understanding the effectiveness of Lithuania's response and the broader implications for migration management in the Baltic region. The phenomenon of weaponized migration, particularly evident in the Lithuania-Belarus border crisis, challenges existing legal frameworks designed to protect asylum seekers' rights. As states face unprecedented pressures from hybrid threats involving both state and non-state actors using migration as a geopolitical tool, the responses to these crises raise important concerns about compliance with human rights standards.

C. The Lithuania-Belarus border crisis: a case study of hybrid migration tactics

The crisis of the border of Lithuania-Belarus emerged as a significant focal point in European geopolitics, mainly due to the strategically used hybrid migratory tactics by the Belarusian government. The genesis of this crisis can be traced back to the growing tensions between Belarus and the European Union, in particular following the controversial presidential elections in Belarus in 2020. As Filipec indicates [29], the Belarusian regime has resorted to political pressure to eliminate the political pressure for the EU political pressure. By facilitating the movement of these individuals towards the EU boundaries, the Belarusian government aims to create a humanitarian crisis that underlines vulnerability and divisions within the EU.

The occupation of these hybrid migration tactics can be interpreted as a form of hybrid war, in which irregular methods are used to challenge traditional security paradigms. Berzins [30] elaborates the way in which this approach effectively obscures the boundaries between war and peace, incorporating elements of political, economic and social dimensions to create instability without working in the conventional military clash. In this context, migration becomes a weapon, a means to destabilize neighboring countries and cause a national and international response from the EU. The Belarusian government has not only facilitated the entry of migrants but has also taken direct actions, such as orchestrating their movement towards the borders, which creates a pressure of humanitarian discomfort and political crisis. It is important to underline that the implications of armed migration extend beyond the immediate context of the control of borders and humanitarian aid; They resonate deeply in the framework of regional security and international relations. The tactics employed by Belarus reflect a wider strategy designed to exploit vulnerabilities within the EU's political scene. The EU's response to this hybrid threat includes the strengthening of border defenses, which, according to Lubbiński [31], risks perpetuating a cycle of aggression and growing tensions between the EU and Belarus. Lithuania, as a first-line state, is in a precarious position, which requires a balance between humanitarian obligations with those looking for a refuge and the imperative to safeguard national security. As noted by Filipec [29], the influx of migrants not only contested the domestic resources of Lithuania, but has also sought relationships with its EU partners and neighboring

countries. The crisis has catalyzed discussions on the collective responses of the EU to the challenges of migration, increasing the awareness of the need for a cohesive immigration policy and the safety paintings of the borders within the EU.

Lithuania's migration management was governed by a complex legal framework shaped by both national legislation and EU laws. As an EU member since 2004, Lithuania is bound by the Common European Asylum System (CEAS). However, in response to the migration crisis, Lithuania implemented numerous state of emergency measures, allowing for the introduction of border controls and restrictions on asylum applications. Filipec [29] notes that these legal changes, presented as essential for national security, have raised concerns about their compliance with international obligations, particularly under the 1951 Refugee Convention and the European Convention on Human Rights.

Lithuania‘s response to irregular migration, especially following provocations by the Belarusian government, has also involved greater cooperation with other EU member states to enhance border security and establish a unified stance against hybrid threats. The collaboration between the Baltic States - Lithuania, Latvia, and Estonia - and Frontex, the European Border and Coast Guard Agency, is a key example of Lithuania’s proactive approach to maintaining regional stability and addressing the migration challenge. This joint effort not only strengthens the capabilities of frontline states but also facilitates crucial intelligence sharing, which is vital for combating illegal migration and organized crime.

Additionally, Lithuania has pursued domestic legal reforms aimed at streamlining the asylum process and enhancing the legal support available to asylum seekers, despite the hybrid nature of the crisis. According to Filipec [29], these reforms represent a dual obligation: ensuring national security while upholding Lithuania's commitments as an EU member and as part of the international community. This balancing act highlights the complexities of managing migration at the border and underscores the need for a flexible legal framework capable of addressing hybrid threats without undermining human rights standards, while also meeting political expectations at both the national and international levels.

Initially, irregular migration from Belarus into Lithuania was relatively limited in early June 2021, but the numbers escalated sharply in July. By early August 2021, over 4,000 individuals had crossed the border irregularly. Between June 2021 and January 1, 2022, Lithuania registered a total of 4,326 irregular migrants, of whom 72% were men and 28% were women. Additionally, 25% of all migrants were minors, including over 500 children under the age of nine. The majority of these individuals entered Lithuania before August 11, 2021, when the Lithuanian Ministry of the Interior issued an order to deny entry and implement pushbacks for all irregular migrants attempting to cross from Belarus [32]. On November 10, 2021, Lithuania declared a state of emergency, imposing significant restrictions on access to the border region. These restrictions applied to journalists and humanitarian organizations, including those providing medical assistance. Furthermore, in December 2021, Lithuania introduced amendments to its migration policy, affecting the rights of migrants and the conditions within camps and detention facilities. Under the revised legal framework, migrants with pending or rejected asylum applications could be detained for up to one year. Since the implementation of pushback policies in August 2021, approximately 8,200 cases of migrants being turned away at the Lithuanian border have been recorded (as of January 23, 2022). The majority of these migrants originate from regions experiencing political, ethnic, and socio-cultural conflicts. These groups include Kurdish minorities from Iraq, Iran, and Syria; the Pashtun minority from Pakistan; and other displaced populations affected by ongoing conflicts in Syria, Afghanistan, and various African nations. Many of these individuals have sought asylum in EU neighboring states, while some have continued their journey toward EU member countries in search of protection and stability [33].

In addition, nearby Poland has undergone similar challenges due to the increase in migratory flows orchestrated by the Belarusian regime. The response of the Polish government included a militarization of the border, with thousands of troops deployed to prevent violations and maintain safety. This response reflects a wider trend of moving from humanitarian assistance to a militarized border management approach [34]. This shift raises concern within the EU regarding compliance with international human rights obligations and the long-term sustainability of these strategies, in particular, public discourse that asks for a balanced approach that considers the rights and needs of migrants while guaranteeing state security.

The interaction between external pressures and internal responses highlights the complexity of national and EU-level security in the face of state-sponsored hybrid tactics. The discourse surrounding the crisis at the Lithuania-Belarus border reflects a significant erosion of asylum rights, as the countries involved respond to the crisis with increasingly restrictive measures. Belarus's use of hybrid migration tactics to exploit vulnerabilities in the asylum systems of neighboring states has prompted a reevaluation

of established protocols concerning the rights of refugees and asylum seekers. Ancite-Jepifánova [35] argues that the tactics employed by Belarus, particularly the orchestrated facilitation of irregular migration flows, compel the affected nations to adopt measures that restrict access to asylum. These developments suggest a growing trend toward the securitization of migration policies, where national security concerns take precedence over international human rights obligations. According to Broks et al. [36], this crisis has catalyzed a series of legislative changes in states such as Lithuania, Poland, and Latvia, driven by the need to mitigate the perceived threats associated with irregular migration. These changes include accelerated deportation procedures, increased border patrols, and provisions allowing the refusal of asylum requests at the borders. These legal alterations undermine the principle of non-refoulement, which stipulates that individuals should not be returned to countries where they face serious threats to their life or freedom.

These measures have sparked significant criticism from human rights organizations and advocates, who argue that these actions may contravene states' obligations under international law, particularly the 1951 Refugee Convention and subsequent Human Rights Treaties. By normalizing a narrative that equates irregular migration with threats to security, states risk eroding the fundamental principles that ensure protection and assistance for those fleeing danger. As articulated by Mitchel & Pratt [37], the normalization of restrictive measures based on security concerns poses a serious risk not only to those affected by these policies but also to the integrity of the broader human rights framework.

Nations such as Lithuania have justified stringent border checks by framing their actions as necessary for national security, a logic that could potentially set a precedent for future actions between EU Member States. The growing polarization between states willing to support the rights of asylum seekers and those prioritizing border security may exacerbate existing tensions within the EU, challenging the principles of solidarity and shared responsibility that underpin migration policies.

As the crisis evolves, the effects of the hybrid migration tactics employed by Belarus are likely to continue reverberating throughout the region, prompting a critical examination of both national and international migration policies. The delicate balance between ensuring national security and adhering to international human rights norms requires careful and informed policymaking. The adoption of a security-first approach risks not only undermining the protection of refugees and asylum seekers but also reshaping the discourse around mobility in ways that could have long-lasting negative implications for global asylum systems and the protection of vulnerable populations.

The legal and political ramifications of the Lithuania-Belarus border crisis highlight the urgent need for a re-evaluation of how countries respond to hybrid migration tactics. The path chosen by these nations raises significant concerns about the future of asylum rights, the effectiveness of international legal frameworks, and the potential for increased bilateral and multilateral tensions in the face of evolving security challenges. The stakes involved underscore the importance of maintaining a commitment to international human rights standards, particularly in the face of complex geopolitical challenges that test the resilience of asylum and migration systems. As elucidated by Kaźmierczak & Laskowski [38], the crisis exemplifies the strategic use of migration as a tool to exploit vulnerabilities in the EU's political and legal structures. Belarus, under the regime of Alexander Lukashenko, has actively weaponized migration, orchestrating the entry of thousands of migrants into Lithuania as a form of hybrid warfare. This tactic serves as a pressure point, compelling the EU to reassess its approach to migration, not only through the lens of humanitarian obligations but also in terms of national security and stability.

The implications of such regional security tactics are profound. Mészáros & Țoca [39] argue that the manipulation of migratory flows destabilizes not only border states like Lithuania but also the entire EU, fundamentally altering perceptions of sovereignty. This emerging threat complicates traditional notions of state sovereignty, as existing security paradigms prove increasingly insufficient to address the fluid and dynamic nature of hybrid threats, which blur the lines between war, humanitarian crises, and diplomacy. The EU must confront the reality that its borders have become arenas for power struggles, where the distinction between military and non-military actions is increasingly obscured.

We can examine one case as an example of the complexity of the situation [40]. In the summer of 2021, Sajjad M, an Iraqi national, was among the first asylum seekers to enter Lithuania via Belarus, seeking protection in the European Union. His journey was part of a broader wave of people fleeing the Middle East and Sub-Saharan Africa, encouraged by Belarus's declared opening of a migration route into the EU. Lithuania's reaction to this influx of migrants, particularly from Belarus, was swift and stringent. The state declared a state of emergency, imposed mass pushbacks, denied effective access to asylum, and subjected thousands of asylum seekers to detention. Sajjad M was one of those detained, remaining

in custody for almost a year under harsh conditions. This case has become emblematic of Lithuania's response to the 2021 crisis and the legal challenges it raised regarding human rights and asylum procedures. Upon his arrival in Belarus in the summer of 2021, Sajjad M made his way to the Lithuanian border, where he expressed his intent to seek asylum. However, instead of receiving assistance or being allowed to file his asylum application, he was detained. He was handcuffed and immediately transferred to the Druskininkai detention center, a makeshift facility used to house asylum seekers under Lithuania's emergency measures. Over the next year, Sajjad was transferred between three different detention sites, each more restrictive than the last, with conditions that fell far below the standards set by both EU and international human rights law.

Sajjad M's detention was marked by brutal treatment and appalling conditions. At the Druskininkai camp, which was originally an improvised facility, he was subjected to overcrowded tents, unsanitary conditions, and inadequate access to basic necessities like clean water and proper sanitation. These dire conditions were repeated at subsequent detention sites, including the Kybartai detention facility, which was a repurposed prison. Kybartai featured high concrete walls, barbed wire, and restricted access to essential services. In one instance, Sajjad was placed in solitary confinement in an isolation cell, with barred windows and heavy metal doors, conditions that further exacerbated his psychological distress.

Sajjad's suffering was compounded by violent treatment by Lithuanian authorities. During one attempted escape from the second detention center, he was subjected to pepper spray and a dog attack that left him with severe injuries. He was further subjected to physical abuse, being beaten after his return to detention. These actions by Lithuanian officials not only violated international norms but also directly contravened the rights of asylum seekers under European law.

Sajjad M's experiences led him to file an application to the European Court of Human Rights (ECtHR) in June 2022 while still detained in Lithuania. He alleged multiple violations of the European Convention on Human Rights (ECHR), including unlawful detention under Article 5, as well as inhumane and degrading treatment under Article 3. His claims were grounded in the unlawful nature of his detention, the physical abuse he endured, and the deplorable conditions in the detention centers. Additionally, Sajjad argued that he was deprived of any effective remedy or legal recourse, violating his rights under the ECHR.

The influx of migrants through Belarus in 2021 was part of a broader political strategy by the Belarusian government under Alexander Lukashenko. The Belarusian authorities, in an apparent effort to destabilize the European Union, facilitated the movement of large numbers of people from the Middle East and Sub-Saharan Africa toward the EU's eastern borders. Lithuania, along with neighboring Poland and Latvia, responded by adopting emergency measures that included mass pushbacks, arbitrary detention, and the rejection of asylum applications through expedited procedures that lacked transparency and fairness.

NGOs reported widespread human rights abuses, including harassment, forced returns, and violence at border areas. The conditions in detention facilities were also substandard, with inadequate medical care and insufficient access to legal support. Asylum seekers were frequently denied adequate interpretation, information about their legal rights, or access to meaningful legal representation, leading to the rejection of asylum claims through sham procedures.

In 2022, the European Court of Justice ruled that Lithuania's mass returns and automatic detention regime violated EU law. However, this legal ruling came in the context of the EU's broader crisis response, which involved the creation of the crisis and force majeure regulation. This regulation, in part, responded to the situation at the Lithuanian-Belarus border and allowed member states to delay registration and access to asylum procedures in the event of a "mass influx of third-country nationals," a term that was intended to address perceived threats from Belarus's facilitation of irregular migration.
While the European Court of Justice's ruling reaffirmed the importance of adhering to EU asylum standards, it highlighted the growing tension between national security concerns and human rights obligations. Lithuania's legal reforms, designed to combat irregular migration, came under scrutiny for violating asylum seekers' fundamental rights. This case exemplifies the complex intersection of national security, migration policy, and human rights within the EU.

Sajjad M's case against Lithuania before the European Court of Human Rights exemplifies the severe consequences of hybrid migration tactics and the legal and human rights violations that can result when states prioritize security over the protection of asylum seekers. His treatment at the hands of Lithuanian authorities raises critical questions about the application of European and international human rights standards in times of crisis. The legal proceedings surrounding this case will have significant implications for future asylum practices in the EU, especially in the context of hybrid warfare tactics that

exploit vulnerabilities in the EU's legal and political systems. The ongoing challenge posed by the Lithuania-Belarus border crisis underscores the need for a comprehensive and rights-respecting approach to migration that balances security concerns with the fundamental rights of refugees and asylum seekers.

IV. CONCLUSIONS

In summary, the border crisis between Lithuania and Belarus highlights the complexities of modern security dilemmas. The adoption of hybrid migration tactics by the Belarusian government serves as a clear reminder of how irregular warfare strategies can profoundly influence regional stability and international relations, necessitating nuanced and coordinated responses from the EU and its Member States. The implications of these tactics on regional security are far-reaching, affecting not only Lithuania but also the internal stability and external borders of the European Union. The use of hybrid migration tactics by the Belarusian government has led to an unprecedented surge in irregular migration flows, presenting significant security challenges for neighboring states.

As the situation evolves, the European Union is compelled to respond to these hybrid threats, balancing its humanitarian values with the imperative to maintain both internal and external security. Gatta [41] insights illustrate that the EU has been forced to re-evaluate its policies on irregular migration in the context of hybrid warfare. Existing frameworks to address migration challenges have often been reactive rather than proactive, focusing on immediate crisis management rather than long-term strategic solutions. The EU's approach must adapt to foster collaborative efforts involving all Member States, as the security of the region is intrinsically interconnected. Without such collaboration, the security situation at the borders of Lithuania and Poland may be exacerbated, potentially destabilizing the EU's internal cohesion regarding migration and border policy. This could lead to divergent responses among Member States, further complicating the crisis.

In addressing political responses to manage these hybrid threats, it is crucial to recognize the duality of security and humanitarian considerations. Yeliseyeu [42] emphasizes the need for a comprehensive approach that integrates border security measures with humanitarian assistance and legal avenues for asylum seekers. Recommendations may include establishing integrated border protection structures capable of providing rapid-response resources and ensuring humane treatment of individuals at the border. This dichotomy presents both a challenge and an opportunity for the EU to redefine its role within the changing geopolitical landscape.

Finally, the Lithuania-Belarus border crisis catalyzes a broader conceptual shift from rigid national security paradigms to a more nuanced understanding that incorporates hybrid threats. This shift requires cooperative strategies and recognizes the complexities of today's humanitarian challenges. As the crisis continues to unfold, the lessons learned will be crucial in shaping future dynamics of international relations, guiding states in navigating the intersection of sovereignty and humanitarian imperatives.

REFERENCES

[1] Ministry of Foreign Affairs of the Republic of Lithuania. At the OSCE Permanent Council, Lithuania condemns Belarus for artificially creating migration crisis, July 30 2021. [Online]. Available: https://www.urm.lt/en/news/928/at-the-osce-permanent-council-lithuania-condemns-belarus-for-artificially-creating-migration-crisis:34708 [Accessed: March 10, 2025].

[2] Migrants Find New Path to EU as Lithuania Plugs Belarus Border. Bloomberg, August 6, 2021. [Online]. Available: https://www.bloomberg.com/news/articles/2021-08-06/migrants-enter-eu-via-poland-as-lithuania-plugs-belarus-border?embedded-checkout=true [Accessed: March 10, 2025].

[3] Republic of Lithuania Law on the Legal Status of Foreigners. 29 April 2004 No IX-2206. As last amended on 17 March 2022 – No XIV-946. [Online]. Available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/ac2cfa50b06f11ecaf79c2120caf5094 [Accessed: March 10, 2025].

[4] Council of Europe. Legal challenges related to hybrid war and human rights obligations, Committee on Legal Affairs and Human Rights, Rapporteur: Mr Boriss Cilevičs. 2016. [Online]. Available: https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24547&lang=en [Accessed: March 10, 2025].

[5] B. Pranevičienė and V. Vasiliauskienė, Hybrid Threats to Energy Security: Perspectives of International Law, Czech Yearbook of Public and Private International Law, Vol. 10, 2019, pp. 74-90. [Online]. Available: https://rozkotova.cld.bz/rww/CYIL-vol-10-2019. [Accessed: March 10, 2025].

[6] F. Bekkers, R. Meessen, and D. Lassche. Hybrid Conflicts: the New Normal? TNO: Innovation for Life. 2019. [Online]. Available: https://www.tno.nl/publish/pages/7427/tno-2019-hybride.pdf . [Accessed: March 10, 2025].

[7] S. Sanz-Caballero, "The concepts and laws applicable to hybrid threats, with a special focus on Europe". Humanities and Social Sciences Communications, 10, 2023. [Online]. Available: https://doi.org/10.1057/s41599-023-01864-y . [Accessed: March 12, 2025].

[8] F. G. Hoffman. Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies. 2007. [Online]. Available: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf [Accessed: March 12, 2025].

[9] J. Grygiel and A. W. Mitchell. The Unquiet Frontier: Rising Rivals, Vulnerable Allies, and the Crisis of American Power. Princeton University Press, 2017. DOI:10.1515/9781400888139

[10] M. Hanssen. Russian Hybrid Warfare: A Study of Disinformation. Journal of Strategic Studies. 2018. [Online].

Available: https://www.econstor.eu/bitstream/10419/197644/1/896622703.pdf . [Accessed: March 12, 2025].
[11] M. J. Mazarr. Hostile Social Manipulation: Present Realities and Emerging Trends. *RAND* Corporation. 2019. [Online]. Available: https://www.rand.org/pubs/research_reports/RR2713.html. [Accessed: March 10, 2025].
[12] N. Popescu. Hybrid tactics: Russia and the West. 2015. [Online]. Available: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_46_Hybrid_Russia.pdf [Accessed: March 10, 2025].
[13] Ministry of Foreign Affairs of the Russian Federation, The Concept of the Foreign Policy of the Russian Federation approved by Decree of the President of the Russian Federation V. Putin on 31 March 2023, No. 229. [Online]. Available: https://theatrum-belli.com/wp-content/plugins/pdfjs-viewer-shortcode/pdfjs/web/viewer.php?file=https://theatrum-belli.com/wp-content/uploads/2023/04/2023_03_31_The-Concept-of-the-Foreign-Policy-of-the-Russian-Federation.pdf&attachment_id=339368&dButton=true&pButton=true&oButton=false&sButton=true [Accessed: March 10, 2025].
[14] Ministry of Foreign Affairs of the Russian Federation, The Concept of the Foreign Policy of the Russian Federation approved by Decree of the President of the Russian Federation V. Putin on 12 February 2013, No. 303. [Online]. Available: https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/Concept_of_the_Foreign_Policy_of_the_Russian_Federation_2013.pdf). [Accessed: March 10, 2025].
[15] M. Galeotti. 'Hybrid War' and 'Little Green Men': How It Works, and How It Doesn't. In Pikulicka-Wilczewska, A. & Sakwa, R. Ukraine and Russia: People, Politics, Propaganda and Perspectives. E-International Relations Publishing. 2015. [Online]. Available: https://www.e-ir.info/publication/ukraine-and-russia-people-politics-propaganda-and-perspectives/ [Accessed: March 10, 2025].
[16] M. Kofman and M. Rojansky. A Closer look at Russia's "Hybrid War*"*. Wilson Center. Kennan Institute. 2015. [Online]. Available: https://www.wilsoncenter.org/sites/default/files/media/documents/publication/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf. [Accessed: March 15, 2025].
[17] P. Pomerantsev and M. Weiss. The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money. A special report. A project of the Institute of Modern Russia, pp.1-44. 2014. [Online]. Available: https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf [Accessed: March 10, 2025].
[18] O. Fridman, 'The Russians are Coming': The Politicisation of Russian Hybrid Warfare', Russian "Hybrid Warfare": Resurgence and Politicization, Oxford Academic, 21 February 2019. [Online]. Available: https://doi.org/10.1093/oso/9780190877378.003.0007 [Accessed: March 10, 2025].
[19] N. Nilsson. Between Russia's 'Hybrid' strategy and Western Ambiguity: Assessing Georgia's Vulnerabilities, *The Journal of Slavic Military Studies*, 34:1, pp. 50-68, 2021. [Online]. Available: https://doi.org/10.1080/13518046.2021.1923992. [Accessed: March 10, 2025].
[20] J. Watling and O. V. Danylyuk, and N. Reynolds. Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War, February 2022 – February 2023. Special Report, Royal United Services Institute for Defence and Security Studies. pp.1-39. 29 March 2023. [Online]. Available: https://rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-russias-unconventional-operations-during-russo-ukrainian-war-february-2022. [Accessed: March 10, 2025].
[21] A. Mumford and P. Carlucci. Hybrid warfare: The continuation of ambiguity by other means. European Journal of International Security. Volume 8, Issue 2, pp. 192-206. 2023. [Online]. Available: https://www.cambridge.org/core/journals/european-journal-of-international-security/article/hybrid-warfare-the-continuation-of-ambiguity-by-other-means/1B3336D8109D418F89D732EB98B774E5. [Accessed: March 10, 2025].
[22] K. Pynnöniemi and M. Jokela. Perceptions of hybrid war in Russia: means, targets and objectives identified in the Russian debate. Cambridge Review of International Affairs, *33*(6), 828–845. 2020. [Online]. Available: https://doi.org/10.1080/09557571.2020.1787949 [Accessed: March 10, 2025].
[23] I. Surwillo and V. Slakaityte. Fortifying the EU's eastern border countering hybrid attacks from Belarus. Surveillance technology and physical barriers secure EU's Eastern border. 4 March 2022. [Online]. Available: https://www.diis.dk/en/research/fortifying-the-eus-eastern-border-countering-hybrid-attacks-from-belarus [Accessed: March 10, 2025].
[24] P. Pomerantsev Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia. Faber & Faber, 2019.
[25] E. Kużelewska and A. Piekutowska. Belarus' Violation of International Obligations in Connection with Artificial Migration Pressure on the Belarus-European Union Border. Bialostockie Studia Prawnicze, 28, 39. 2023. [Online]. Available: https://doi.org/10.15290/bsp.2023.28.01.03. [Accessed: March 10, 2025].
[26] The 1951 Refugee Convention and 1967 Protocol relating to the Status of Refugees. UNHCR. [Online]. Available: https://www.unhcr.org/media/1951-refugee-convention-and-1967-protocol-relating-status-refugees. [Accessed: March 10, 2025].
[27] Seimas of the Republic of Lithuania Resolution on Declaration of a State of Emergency, 7 December 2021 No XIV-733. [Online]. Available at: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/37e55ab258dc11ecacf0d54306d0ca27?jfwid=mbn9t1bmz [Accessed: March 10, 2025].
[28] Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (recast), OJ L 180, 29.6.2013, pP. 60–95, [Online]. Available: http://data.europa.eu/eli/dir/2013/32/oj [Accessed: March 10, 2025].
[29] O. Filipec. Multilevel analysis of the 2021 Poland-Belarus border crisis in the context of hybrid threats. Central European Journal of Politics, 8 (1), pp. 1-18, 2022. [Online]. Available: DOI:10.24132/cejop_2022_1. [Accessed: March 10, 2025].
[30] V. Berzins. Hybrid warfare: weaponized migration on the eastern border of the EU?. The Interdisciplinary Journal of International Studies, 12(1), pp. 19, 2022. [Online]. Available: https://doi.org/10.5278/ojs.ijis.v12i1.6992 . [Accessed: March 10, 2025].
[31] P. Łubiński. Hybrid warfare or hybrid threat–the weaponization of migration as an example of the use of lawfare–case study of Poland. Polish Political Science Yearbook, 51 (1), pp. 43-55. 2022. [Online]. DOI:10.15804/ppsy202209. [Accessed: March 10, 2025].
[32] Ministry of the Interior of the Republic of Lithuania, 2022. [Online]. Available: https://www.lrt.lt/en/news-in-english/19/1864010/lithuanian-cabinet-endorses-controversial-migrant-pushback-legislation?srsltid=AfmBOoqdGHYolSWEQ9q7sHF2tVkH6zw_Jw1VojcSnMrLAJQxckhtWm8C. [Accessed: March 10, 2025].

[33] OHCHR, Report. April 2022. [Online]. Available: https://www.ohchr.org/sites/default/files/2022-04/SienosGrup%C4%97Submission.pdf. [Accessed: March 10, 2025].

[34] G. Baziur. Operation "Sluice". The so-called migration crisis at the Polish-Belarussian border: an example of hybrid actions taken in the second half of 2021 as documented in the reports of the Polish border guard. Bezpieczeństwo. Teoria i Praktyka, 46(1), pp. 133-150, 2022. [Online]. Available: https://orcid.org/0000-0001-6652-8981 . [Accessed: March 10, 2025].

[35] A. Ancite-Jepifánova. Beyond the "Hybrid Attack" Paradigm: EU-Belarus Border Crisis and the Erosion of Asylum-Seeker Rights in Latvia, Lithuania and Poland. AVANT. Pismo Awangardy Filozoficzno-Naukowej, (2), pp. 1-26, 2024. [Online]. DOI:10.25360/01-2024-00007. [Accessed: March 10, 2025].

[36] E. Broks, A. Buka, L. Buka, and A. Kučs. Limiting the Right to Access Asylum: A Case Study of Latvia's Response to the Migration Crisis on the Latvia-Belarus Border. Baltic Yearbook of International Law 22(1), pp. 201-232, 2024. [Online]. Available: DOI:10.1163/22115897_02201_010 [Accessed: March 10, 2025].

[37] K. Mitchell and T. Pratt, T. Migration-Based. Hybrid Warfare on Europe's Externalized Borders: Case Studies on Morocco and Belarus in 2021. Yale University. 2022. [Online]. Available: https://politicalscience.yale.edu/sites/default/files/keiran_mitchell.pdf [Accessed March 10, 2025].

[1] D. Kaźmierczak and M. Laskowski Social Cohesion in Hybrid Conflicts. Cases of Migration Crisis at the Polish-Belarussian Border and Migration Flows From Ukraine. Przegląd Wschodnioeuropejski, 15(2), pp. 117-129, 2024. [Online]. Available: https://doi.org/10.31648/pw.10868 [Accessed: March 10, 2025].

[2] E. L. Mészáros and C. V. Ţoca. The EU's resilience and the management of hybrid threats coming from the Eastern neighbourhood: Belarus and the deliberate facilitation of irregular immigration. Eastern Journal of European Studies, 14(1), 2023. [Online]. Available: https://doi.org/10.47743/ejes-2023-0101 . [Accessed: March 10, 2025].

[3] ECCHR. Lithuania's illegal detention of asylum-seekers European Court of Human Rights to rule, 2022. [Online]. Available: https://www.ecchr.eu/en/case/lithuanias-illegal-detention-of-asylum-seekers/. [Accessed: March 10, 2025].

[4] F. L. Gatta. The migration crisis goes East: the EU's Eastern borders under strain, between hybrid attacks, threats to human rights and the Ukrainian exodus. 2022. [Online]. Available: http://hdl.handle.net/2067/49850. [Accessed: March 10, 2025].

[5] A. Yeliseyeu. Belarus's Coercive Engineered Migration Case of 2021–2022: Categorisation of State Media Narratives. Studia Migracyjne-Przegląd Polonijny, (3), pp. 79-99, 2023. [Online]. Available: DOI:10.4467/25444972SMPP.23.030.19145 [Accessed: March 10, 2025].

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 237-246

Methods for Description, Analysis and Evaluation of Command and Control Systems (C2)

Ivo G. Radulov
Rakovski National Defence College
Defence Advanced Research Institute
Sofia, Bulgaria
i.radulov@rndc.bg

Abstract- **Every organization needs a clear understanding of its own processes, capabilities, products, technologies and relationships to effectively deliver its objectives in response to a changing environment. A clear understanding of the nature of management systems requires an integrated abstract representation of their multifaceted aspects through organisational modelling methods. When the system is complex, an approach that can provide a unified medium for representing all major functional and system perspectives is necessary for its comprehensive modelling. The purpose of this publication is to present an approach that provides an integration into one environment of organizational goals; policies, concepts, and doctrines; management systems; decision-making procedures; organizational structures, processes, information flows, and data; resources, capabilities, and technologies. In this approach, architecture refers to the fundamental organization of a system, which includes the system components, their relationships with each other and with the environment, and the principles that underlie system design and its development.**

Keywords- Modelling and analysis methods, Modelling, Simulation, Analysis, Evaluation.

I. INTRODUCTION

Command and control systems are complex systems, of the "system of systems" type, whose integrity is a determinant of their overall effectiveness. Their specific characteristics determine the need to establish a clear basis, uniform standards and full integration of all activities and tasks to achieve the set objectives. Ensuring this explicit necessity requires encompassing the entire Command and control system in a single cognitive paradigm. An approach where individual fragments of the 'big picture' are modelled and analysed with different, purpose-built tools is possible. However, achieving compatibility of the respective models may be problematic, given the complex and heterogeneous nature of these systems, including their elements and system relationships. A universal approach is needed to provide a common, integrating basis for system modelling in security and defence [1].

The architectural approach is precisely the means by which the following can be integrated into an environment: 1) objectives; 2) policies, concepts and doctrines; 3) leadership, Command and control systems; 4) planning systems; 5) decision-making procedures; 6) organizational structures, processes, information flows and data; 7) resources, capabilities and technologies [1].

In this approach, architecture is understood as the fundamental organization of a system, which includes the system design with its components, the interrelationships among the components, and the relationships with external organizational systems that correspond to the subject matter of the system under study. Organizational architecture (OA) provides the mechanism that accomplishes the communication between the elements of the organization and its functioning [2].

The conceptual difference in approaches to building organizational architectures is materialized in the way each architecture is formalized. The relevant formalisation tool is the so-called Architecture Framework (AF). The AF provides a single formalized model containing the requirements of C2 systems. The AF is a specification of how to organize and represent the structure of a system, its processes, the capabilities it must have, the technologies, etc. It is a meta-model that ensures compatibility of the models being developed by defining rules, guidelines and product descriptions for their development, representation and communication.

Historically, the first AF is that of Zachman. According to Zachmann, the model for describing systems is built at

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8475
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

the contextual, conceptual and logical levels and illustrated with a matrix. The framework requires answering the questions "what", "how", "where", "who", "when" and "why" from different perspectives to describe the same process. Zachman pulsed a rapid and productive process of developing different AFs and powerful software packages to support them. The type and choice of a particular framework depends on the goals and characteristics of the organization [3].

There are other AFs. In 2003, the U.S. Department of Defence approved the DODAF Architecture Framework, which provides a common integrative approach for modelling and analysis across the U.S. armed forces. The UK MODAF and NATO NAF AFs have been developed based on it [4].

Several AFs incorporate description methods and techniques to assist analysts in reaching an optimal or near-optimal solution to a complex problem. These techniques may include, for example, the Computer Integrated Open Systems Architecture (CIMOSA), the Integrated Definition Engine (IDEF) methodology, Petri nets and their variations, the Unified Modelling Language (UML), organizational function diagrams (EFD), etc. Using these techniques, a clear representation of the processes is achieved through a set of decomposed activities with corresponding inputs, outputs and actors. Some description methods can also represent process dynamics.

Formal description and analysis methods can be conventionally classified into three groups: 1) state machine methods; 2) languages for programming and specification; and 3) combined methods.

State machines. Methods in this group are based on sets of states, performing processing in response to events leading to a state change. These models are a convenient and natural way of describing interactions, but when described in sufficient detail lead to an unacceptably large number of states. These include Petri nets, finite automata, state diagrams, formal grammars, etc.

Languages of description and specification. Methods from the group of programming and specification languages view an interaction as an algorithm and are used to describe it precisely. Their main drawback is that nonessential details can mask important aspects of the interaction of system elements. Algorithm graphschemes, logic schemas, parallel logic schemas, matrix schemas, parallel algorithm matrix schemas, canonical schemas, etc. belong to this group of methods.

Combined methods. The methods of this group integrate the first two groups. The interaction is represented as a machine with a small number of states reflecting the basic features of the interface. This machine is augmented with additional "context" variables and procedures to handle them in each state. The functioning of the machine is determined by the input events, the values of the 'context' variables and the procedures for processing them in the current state. Examples of combination methods are E-networks, Keller's Model, etc.

II. MATERIALS AND METHODS

For the research of a complex Command and control system it is also necessary to define the goals and objectives of the research, to choose the methodological tools for the optimal solution of the set tasks. The toolkit should include quantitative methods, tools for formal description of models, and software products for modelling and simulation. Next, the objective function of the study should be defined. An analytical expression should be chosen to find the overall performance of the system, including the performance indicators. A detailed list of the factors affecting the study object should be prepared. After analysis, the factors essential for modelling shall be identified. The consistency of the selected essential factors with the necessary requirements for the objectives of the study shall be established in order to determine the critical success factors. After these activities, the model/architecture of the existing (As-Is) system is formed. The formed model is subjected to a model controllability check. The activity model (OV-5) has to verification of the adequacy, completeness and inconsistency. The performance of the model is simulated using specialised software tools. The performance of the (As-Is) model is evaluated using the specified objective function. Conclusions and recommendations from the analysis are formed.

The recommendations made are applied to create an advanced model of the desired/future (To-Be) state of the studied system. The new model is again checked for adequacy, completeness and inconsistency where changes have occurred. The performance of the (To-Be) model shall be assessed using a selected modelling and simulation software or appropriate mathematical apparatus. The experiment is usually associated with the influence of critical success factors on the output parameter values. On this basis, the performance of the (To-Be) model is evaluated. The effect of changes is calculated. Conclusions and recommendations are formed.

The results of the study can be interpreted in a specific software application. Usually, specialized modelling software automatically generates an outline of a logical model based on the data (OV-7) for the creation of a future information system of the studied model. Next, descriptions of system interfaces (SV-1) and system functionality (SV-4) are prepared, an overview of the subsystems comprising the information system is provided, and a profile of technical standards (TV-1) is developed. A prototype of the system is developed and tested using a separate methodology.

The presented sequence of abstract steps by stages forms a methodology for modelling, analysis and development of complex organizational systems. The proposed methodology is presented schematically in

Fig.1. Depending on the purpose to be pursued, only Stage 1

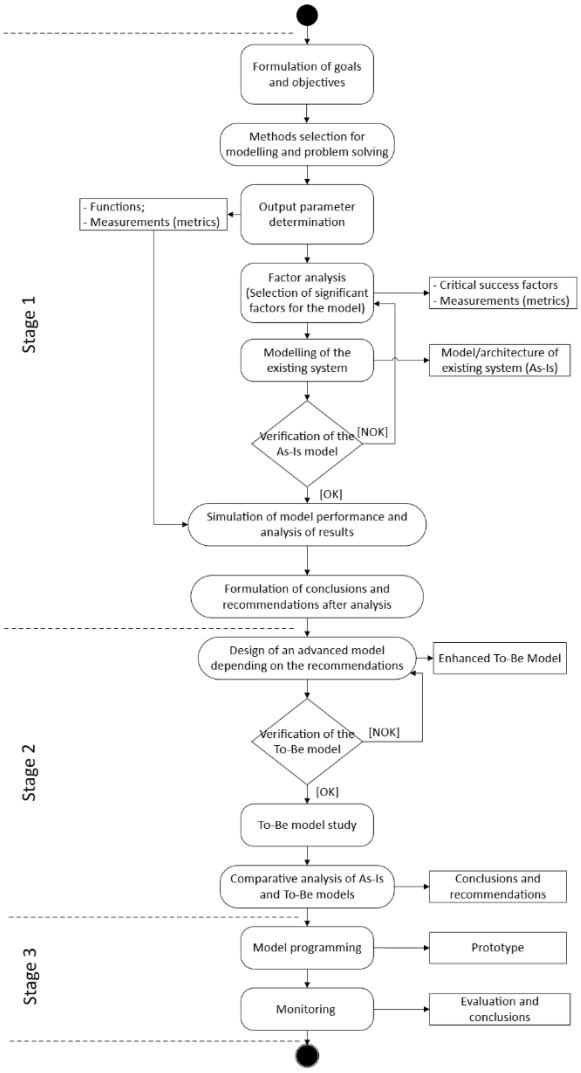


Fig. 1. Methodology for modelling and analysis of complex organizational systems.

for the description of the current system, Stages 1, 2, and 3 or Stages 1 and 3 for the improvement of the existing system can be executed successively.

III. RESULTS AND DISCUSSION

This application is an example of the use of the description and analysis methods described below in the section on the proposed methodology. The research object is the typical C2 system. This is current Capability Planning Subsystem, which is part of the Defence Planning System of the Bulgarian Army. The objective of the study is to increase its effectiveness. The research is a practical expression of the described ideology of the architectural approach. The case study is a sample from the Strategic Defence Review completed in 2020 and presents the status of the Defence Planning System for the period November 2018 to March 2019.

The following approaches were used to find realistic solutions: 1) Architecture Approach with technology of operation described as architecture products as required by the DoD Architecture Framework, Ver. 1.5 document; 2) Process approach, which is based on the concept of Business Process Management (BPM).

The following methods were also used: 1) Scientific Abstraction; 2) Analysis and Synthesis; 3) Modelling; 4) Decomposition; 5) Factor Analysis; 6) Activity Based Costing (ABC); 7) Statistical Modelling and Optimisation Methods.

IDEF0 diagrams were used for the formal description and analysis of the model. Simulation of the model performance was performed using the Ultimus Process Designer Ver. 6.0 software application.

The presented study was performed under the following constraints:

- The creation of the model is based on available normative, regulatory, and reference documents covering the period November 2018 - March 2019;
- Due to the large amount of information, only Stage 1 of the proposed methodology is considered in this paper;
- Information from explicit sources has been used.

In order to simplify the model without significantly changing the modelled environment, the following assumptions are made:

- For the purpose of the study, an approximate accuracy of the results satisfying the analysis is adopted;
- The study is oriented towards increasing the efficiency of the alternatives considered at a given cost - seeking maximum effect;
- It is conventionally assumed that about 300 people are involved in the execution of one cycle of the work of the system, of which about 4% (12 people) are full-time staff, the remaining 288 people are non-regular staff.
- The non-regular staff use about 20% of their working time to carry out planning activities. As a result, for an equivalent full-time workload on an annual basis, about 70 staff work on the implementation of capability planning activities.

Objective function selection

Within the study, performance measurement is oriented towards improving the cost and cycle time performance of the processes at the study site.

Given this, the generalized objective function Y is formed from three output parameters.

$$Y = \phi(y_1, y_2, y_3), \qquad (1)$$

where: Y- subsystem efficiency.

In Tab. 1 are shown the selected output parameters with the relevant outcome indicators and their measures.

TABLE 1 OUTPUT PARAMETERS

***Y* Parameters**	**Performance Indicator**	**Metrics**
y_1	Costs of staff involved in the processes	Euro
y_2	Timeout period (Inactivity time)	Days
y_3	Processing time per task	Hours

The generalized function of the form (1) is sufficiently complex and can be given in the following form [5]:

$$Y = \sum_{v=1}^{u} a_v \cdot y_v,\ u = 2,3 \qquad (2)$$

where a_v are weighting factors that account for the role of individual parameters in the quantitative characterization of the target. They can be positive quantities (when an increase in the corresponding parameter corresponds to the target) and negative quantities (when an increase in the corresponding parameter leads to a move away from the goal).

Because the individual parameters y_1, y_2, y_3 have different physical natures, different dimensions and intervals of definition, the coefficients a_v must also have different dimensions and intervals of variation so that the generalized output parameter has some chosen dimensionality. It is therefore more convenient to proceed to form Y in the form of a dimensionless and bounded in the interval [-1, +1] quantity.

For this purpose, the three parameters y_1, y_2, y_3 are transformed into new parameters $\theta_1, \theta_2, \theta_3$ by the formula [5]:

$$\theta_v = \frac{y_v - \bar{y}_v}{\frac{y_{v,\max} - y_{v,\min}}{2}.u},\ v = 1,2,3, u \le n, \qquad (3)$$

where $\bar{y}_v$ is the average value of y_v, which can be estimated by:

$$\bar{y}_v = \frac{y_{v,\max} + y_{v,\min}}{2}, \qquad (4)$$

The quantities $y_{v,max}$ и $y_{v,min}$ are the maximum and minimum values of y_v, and $u=3$ is the number of parameters that are involved in the formation of the generalized objective function. Then considering (3) and (4) we obtain [5]:

$$Y = \sum_{v=1}^{u} \alpha_v.\theta_v = \frac{1}{3}\sum_{v=1}^{3} \alpha_v \frac{2y_v - (y_{v,\max} + y_{v,\min})}{(y_{v,\max} - y_{v,\min})} \qquad (5)$$

In such a transformation of the individual output parameters, the coefficients α_v can be dimensionless if they are also chosen in the interval [-1, +1], i.e.

$$-1 \le \alpha_v \le 1, \qquad (6)$$

the generalized objective function Y in will be a dimensionless quantity whose values are constrained:

$$-1 \le Y \le 1, \qquad (7)$$

Selection of modelling factors

From a modelling perspective, the Capability Planning Subsystem under study is a multifactorial object incorporating material, human and information resources that is impacted by a number of factors. In order for the model of the studied object to be adequate, the most significant factors determining the functioning of the model must be included in the model. That is, the task of selecting the factors in modelling boils down to identifying the essential factors and eliminating the non-essential factors. In practice, this involves:

1. Preparation of a detailed list of factors impacting the performance of the subsystem under study;
2. Selecting the essential factors and eliminating the non-essential ones;
3. Establishing the compliance of the selected essential factors with the necessary requirements from a modelling perspective.

To facilitate the selection of the significant factors that affect model performance, the factor space is divided into three areas: planning, organizing, and execution. For each of these, a complete list of candidate factors (F_i) (20 in total) required for the formation of the model of the object under study was determined by brainstorming. The selection of the significant factors for the model was performed by the rank correlation method through a survey of 15 highly qualified experts with years of experience in defence planning. After the data processing, the degree of agreement between the experts' opinions was determined using the concordance coefficient (W). The consistency of the opinions was done by formula (8) since the ranking contains matching ranks:

$$W = \frac{S_d}{\frac{1}{12}m^2.n(n^2-1) - m.\sum_{j=1}^{m} U_j}, \qquad (8)$$

where $S_d = \sum_{i=1}^{n}\left[\sum_{j=1}^{m} x_{ij} - \frac{1}{2}m(n+1)\right]^2$. (9)

After performing the appropriate calculations, a high degree of probability was obtained in the consistency of the experts' opinions on the influence of the factors under study. This gives confidence that the selected factors can be used for modelling purposes.

In the following, the factors are presented in a histogram of summary ranks from which the significant factors are separated. Three of the most significant factors are identified from the histogram. These are listed in Table 2. These are identified as the critical factors of the modelling. Once the factors have been selected, their respective metrics and the measurement units by which each should be scaled are established.

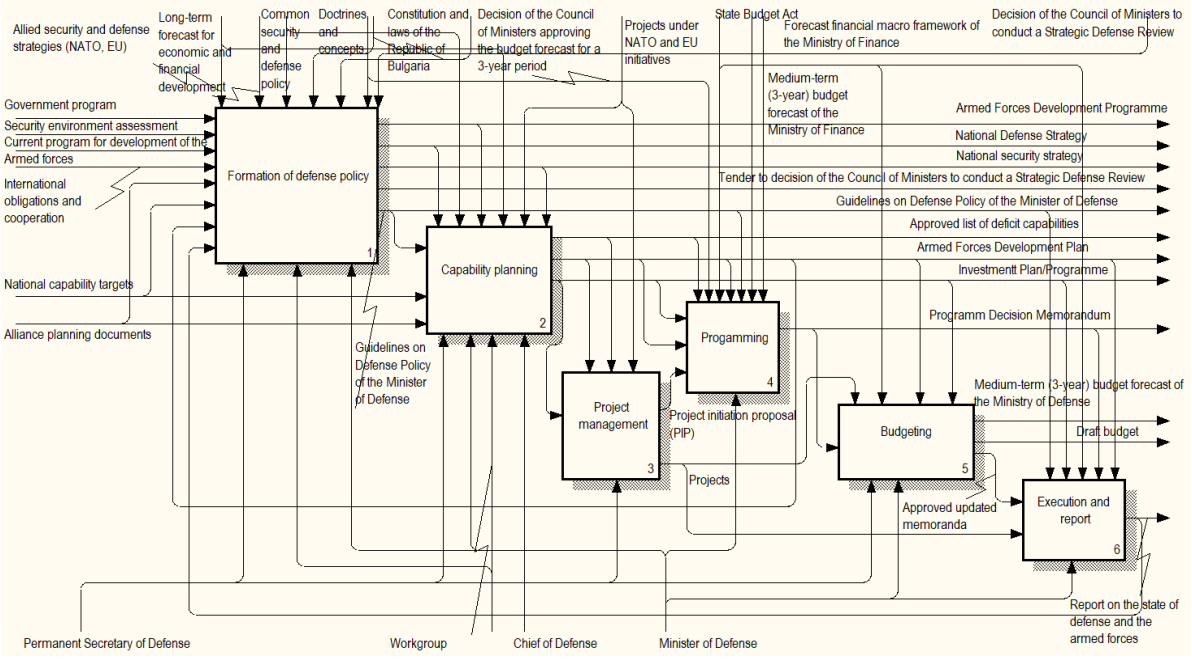


Fig. 2. A0 Defence planning model in the Bulgarian Armed Forces (BAF)

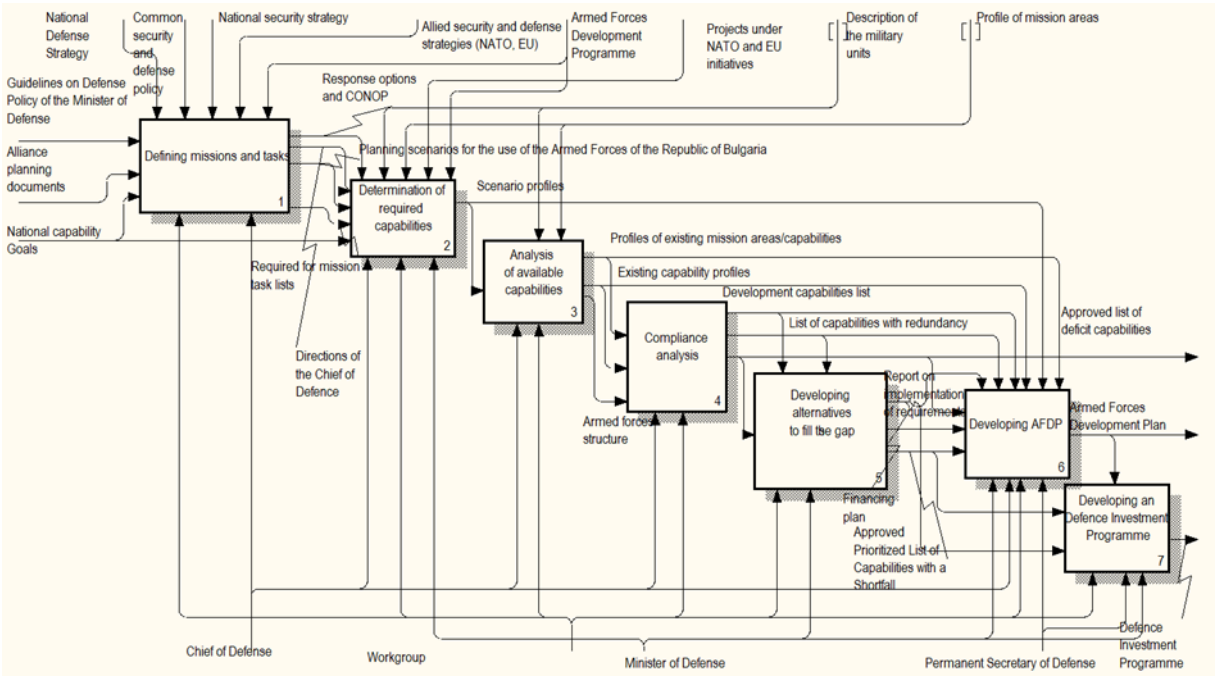


Fig. 3. A2 Capability planning sub model

It is characteristic for the selection of the factors that they must meet the following basic requirements: 1) each individual factor must allow for quantification; 2) they must be controllable; 3) they must be independent, i.e., no two factors are functionally related in the set; 4) they must be consistent, i.e., it must be possible to realize all possible combinations of factor values within their domains of definition [5, 6].

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8475
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

TABLE 2 MOST SIGNIFICANT FACTORS

Factor	Essence of the Factor	Indicator	Metrics
F1	Performance of the participants	Time for completion of individual activities	Hour
F2	Process resourcing, including the human resources (full time and non-full time officials, management staff) of the management and executive structures involved in the processes	Amount of personnel	Number
F3	Funding of activities	Participants' labour costs	Euro/ hour

Activity Model (OV-5)

After determining the objective function and critical factors for the modelling, the As-Is model of the study object is formed.

The activity model is presented in Fig. 2 using CASE system (Computer-aided software engineering) according to IDEF0 standard. To demonstrate the described methodology, the activity diagrams are decomposed to the level two (Fig. 3).

Verification of the adequacy, completeness and inconsistency of the OV-5 activity model

Checking for adequacy, inconsistency and completeness of the model presented in Fig. 3. is the next step that the researcher has to do. The verification is performed using an E-network model of the interaction and matrix properties of the algorithm, see [Radulov I., "Modelling of capability-based defence planning processes, 2024"]. Similarly, the A2 Capability planning submodel presented in Fig. 3 was checked for adequacy. From the verification of transition management and reachability of E-network states, it turns out that all A2 model states are reachable. The consistency and completeness check of A2 was performed using a matrix scheme of the algorithm as described in [7, 8]. The formed model of the capability planning subsystem is proved to be adequate, consistent and complete. The operation as a set of subnetworks was simulated using the Visual Object Net++ Evaluation Version 2.0a software product.

Evaluation of the controllability of the model

At this stage, the impact of the controlled factors on the model output parameter values is evaluated. It is characteristic of multifactor objects, such as the Capability Planning Subsystem under study, that the generalized output parameter *Y* changes significantly under the influence of the factors selected for the study. In some cases, however, the changes in *Y* are insignificant, and it is difficult to determine whether they are due to changes in the controlled factors or to confounding factors. If the influence of the controlled factors is insignificant, the study of the model with them becomes pointless. It is therefore necessary to assess the appropriateness of modelling the process with the selected factors at the outset of the study.

Verification of the controllability of the model was carried out prior to conducting the overall experiment. In this regard, the evaluation was performed for one process state of the As-Is model for a certain number of experiments (n) with different values of the input factors. After each experiment, the values of the objective function parameters were recorded, and their estimates and variance were calculated using the following formulas [5]:

$$\bar{y}_u = \frac{1}{n}\sum_{i=1}^{n} y_{i_u},\ u=1\ldots3 \qquad (10)$$

$$S^2_{y_u} = \frac{1}{n-1}\sum_{i=1}^{n}.\left(y_{i_u} - \overline{y_u}\right)^2, \qquad (11)$$

where $\bar{y}_u$ is the average value of the parameter, and $S^2_{y_u}$ is its dispersion.

The Fisher criterion (F-criterion) was used to compare the dispersion estimates $S^2_{y_u}$ and the dispersion estimate of the equivalent disturbance $S^2_{\varepsilon u}$ for each parameter separately [5].

$$F_u = \frac{S^2_{yu}}{S^2_{\varepsilon u}} \qquad (12)$$

The verification of the considered process was performed under five different combinations of values of the critical factors for which the values of the parameters of the generalized objective function were measured. In order to analyse whether the controlled factors have a significant influence on the model output parameter, the experimental data for $\overline{y}_1$ and S^2_{y1} are obtained as: $\overline{y}_1$=103038,67 и S^2_{y1}= 883889512,25. The experimental results for the remaining parameters are plotted in Table 3.

TABLE 3 THE EXPERIMENTAL RESULTS

i	1	2	3	4	5
y_1	120097,34	145090	91567	89465	68974
y_2	9724,32	8124,02	5534,33	11632,17	4544,53
y_3	17,50	12,00	7,00	5,50	10,50

i	$\overline{y}_j$	$S^2_{y_j}$
y_1	103038,67	26591,57
y_2	7911,87	2613,90
y_3	10,50	4,21

From ten other observations conducted with constant factor values, the estimate of the single dispersion was determined $S^2_{\varepsilon 1}$ = 883889512,3 . The calculated F-coefficient is: $F_1 = \frac{S^2_{y1}}{S^2_{\varepsilon 1}} = \frac{26591{,}57}{2769{,}96} = 9{,}6$.

From a table of reference, the tabular value of the significance of Fisher's criterion was determined. At a significance level of α=0,05 and freedom degrees of

ν_1=5-1=4 and ν_2=10-1=9, for the single dispersion S_{y1}^2 and the dispersion of the equivalent disturbance $S_{\varepsilon 1}^2$, obtained with N observations, respectively, the tabular value of Fisher's criterion is $F_{t1} = F_{t2} = F_{t3} = 6{,}00$. Similarly, $F_2 = \frac{S_{y2}^2}{S_{\varepsilon 2}^2} = \frac{2613{,}90}{348{,}52} = 7{,}5$ and $F_3 = \frac{S_{y3}^2}{S_{\varepsilon 3}^2} = \frac{4{,}21}{0{,}5} = 8{,}4$. Since $F_1 > F_{t1}$, $F_2 > F_{t2}$ и $F_3 > F_{t3}$, the input factors are assumed to significantly affect the parameters of the objective function. Therefore, constructing the model with these factors is reasonable.

Model performance

To find the overall efficiency of the model in (1), it is necessary to determine the cost of the outputs of the capability planning process. For this purpose, the Activity Based Costing method is used. The method gives a more accurate picture of the cost of process outputs by allocating costs based on the activities performed to produce them, rather than the traditional linear cost allocation [9, 10].

In this particular example, after describing the activities in Fig. 3, we proceed to divide the costs by categories of personnel in order to make the metrics (cost drivers) more understandable and accurate.

TABLE 4 AVERAGE DAILY RATE BY CATEGORY OF ACTORS

Average Daily Rate by Category in Euros	MoD		BAF	
	Civilian	Officers	Civilian	Officers
By professional relationship	71,42			
Under an employment contract	45,23		40	
Under the Armed Forces Act		100		90,47

In this case, labour costs are grouped by the categories of officials involved in the implementation of the planning activities. These are shown in Table 4. In addition to the category of actors involved in the process, the table also contains the cost per actor in EUR. The cost of the actors involved in the process has been determined on the basis of indicative values for the average gross monthly remuneration for the Bulgarian Armed Forces (BAF) and the Ministry of Defence (MoD). Labour costs are for an 8-hour working day with an average of 21 days worked per month.

For each activity-cost relationship, the level of relationship, i.e. the costs that are generated by the specific activity, is determined. The allocation of costs to activities is based on the participation of each of the experts in the relevant activities at the relevant rate per day. The number of participants for each activity and the days worked by each participant are also determined. The results are plotted in Table 5.

TABLE 5 LABOUR COSTS

Activity	Staff Category	Rate per Day	Number of Staff	Days Worked	Total (Euro)
A2					**109931,19**
A21 Defining missions and tasks					**17275,2**
	Officers MoD	100	2	10	2000
	Officers BAF	90,47	12	10	10856,4
	Civilian 1 MoD	71,42	1	10	714,2
	Civilian 2 MoD	45,23	2	10	904,6
	Civilian BAF	40	7	10	2800
A22 Determination of required capabilities					**19705,56**
	Officers MoD	100	3	14	4200
	Officers BAF	90,47	10	14	12665,8
	Civilian 1 MoD	71,42	2	14	1999,76
	Civilian 2 MoD	45,23	0	10	0
	Civilian BAF	40	3	7	840
A23 Analysis of available capabilities					**14565,8**
	Officers MoD	100	3	5	1500
	Officers BAF	90,47	12	10	10856,4
	Civilian 1 MoD	71,42	1	5	357,1
	Civilian 2 MoD	45,23	2	5	452,3
	Civilian BAF	40	7	5	1400
A24 Compliance analysis					**10447**
	Officers MoD	100	2	10	2000
	Officers BAF	90,47	12	5	5428,2
	Civilian 1 MoD	71,42	1	10	714,2
	Civilian 2 MoD	45,23	2	10	904,6
	Civilian BAF	40	7	5	1400
A25 Developing alternatives to fill the gaps					**15570,48**
	Officers MoD	100	2	12	2400
	Officers BAF	90,47	10	12	10856,4
	Civilian 1 MoD	71,42	2	12	1714,08
	Civilian 2 MoD	45,23	0	0	0
	Civilian BAF	40	3	5	600
A26					**18463,35**

Developing AFDP	Officers MoD	100	3	15	4500
	Officers BAF	90,47	6	15	8142,3
	Civilian 1 MoD	71,42	2	15	2142,6
	Civilian 2 MoD	45,23	1	15	678,45
	Civilian BAF	40	5	15	3000
A27 Developing an Defence Investment Programme					**13903,8**
	Officers MoD	100	1	20	2000
	Officers BAF	90,47	5	20	9047
	Civilian 1 MoD	71,42	2	20	2856,8
	Civilian 2 MoD	45,23	0	0	0
	Civilian BAF	40	0	0	0

Performance evaluation of the As-Is model

The results of the model performance study were validated using the Ultimus Process Designer, Ver. 6.0. software under the following experimental assumptions:

1. Incoming task norm. For the purpose of the study, it is assumed that a new task appears every 4 hours with a standard deviation of +/-1 hour.

2. An acceptable number of tasks to quantify the process. A value of "100" is assumed for better representativeness of the selection.

3. Preload the system. Determines how many tasks will flow through the system, after the process is initiated, before their normal execution flow level is reached. For this example, a value of "20" is assumed, which means that the first 20 tasks will be excluded since the system has not been previously loaded. The execution of these 20 tasks will not reflect the normal workload of the system. This necessitates that only tasks 21 through 120 be included in the sample of the current statistical model.

4. Resources available to execute the tasks at each stage. Contains the number of participants in the process and the cost of each participant in Euros. The sample data used are shown in Table 4.

5. Time required to complete each task and the deviation from this time. These assumptions are specified individually for each process participant and are embedded in the model work.

6. Type of distribution of incoming tasks in the system. The central limit theorem states that the distribution of a sum of a large number of independent, uniformly distributed random variables tends to a normal distribution. Therefore, it can be assumed that the distribution of flows in statistical models obeys some normal distribution. This determines the choice of the normal distribution of the problems in the present model.

The results obtained for the parameters of the generalized objective function (y_1, y_2, y_3) are presented in Table 6, after simulating the model performance with Ultimus Process Designer, Ver. 6.0.

TABLE 6 THE RESULTS FOR THE PARAMETERS OF THE GENERALIZED OBJECTIVE FUNCTION

Generalized Objective Function Parameters	Min Value	Max Value	Average	Standard Deviation
y_1 – Costs for staff involved in the processes (€)	68974,00	145090,00	104187,42	24410,20
y_2 – Timeout period (Inactivity time) (Days)	4544,53	11632,17	7595,23	2488,98
y_3 – Processing time per task (Hours)	5,50	17,50	10,00	4,00

The evaluation of the model effectiveness is performed using the defined analytical expression (5). The values of the weighting coefficients are determined using expert estimation: α_1 = -1; α_2 = -0,5; α_3 = -0,7. They are substituted in (5), where the value of the generalized output parameter Y = 0.106 characterizing the system performance is obtained.

Conclusions and recommendations from the analysis

This example demonstrates a process improvement approach to the Defence Resource Management System. The approach integrates methodologies for describing, implementing and controlling processes and technologies for their implementation. The recommendations, in the order in which they are proposed, improve the output parameter values.

This approach is applied to improve the processes in the formation of the To-Be model and contributes to increase the overall efficiency of the model. The measures that can be applied to improve the performance of the object of study are:

1. *Reducing support functions.* The reduction of support functions, of actors in the Command and control system is associated with the removal from the scheme of operational nodes of actors with little or no contribution to the system. Reducing redundant links between operational nodes, without compromising system reliability, can be accomplished by linking them, for example, from a hierarchical structure to a topology of another type. A possible solution is the use of a star-type structure. In this case, this type of topology can be implemented with organisational changes or with the adoption of information technology, including an information system and facilities for communication.

2. *Improving the process by reducing the waiting time.* From the simulation with the software, it is found that some of the activities are bottlenecked which slows down the overall process execution in the system. The frequency with which tasks are generated and arrive for

processing from lower levels is too high for the teams at the next levels to handle the workload. To overcome the slowdown, the following measures can be implemented:

- Assign additional staff to carry out the various activities;
- Reduce the number of tasks by changing the rules and specifying that not every task is enforceable;
- Increase the speed of implementation.

The appointment of additional personnel has a significant impact on defence spending, which is not an acceptable solution.

Reducing the number of tasks performed is also not an adequate solution due to the fact that all activities of the model are performed according to The Classic Waterfall Development Model, i.e. they are interdependent and are directly or indirectly linked to each other, since the outputs of one activity are the input for the next. Such an approach to work is normal in a complex process, but there is a risk that if the work of one of the working groups is delayed or if the quality of the outputs is low, these negatives may accumulate in the work of the following groups. On the one hand, ignoring or failing to complete tasks can slow down the work of all subsequent groups, and on the other hand, poor quality intermediate results can "distort" the final results.

Of the following options, the only viable alternative is the third, to increase the processing speed. Without changing the work rules and the number of staff, increasing the speed of processing can be done by introducing a complex of measures, including: 1) increasing the qualification of the staff; 2) increasing the methodological guidance of the staff; 3) ensuring the interchangeability of staff; 4) creating additional conditions for parallel work; 5) reducing the time documents stay in the registry system and the time they take to reach the final recipient.

3. *Improving the process by reducing the waiting time.*
From the simulation, it can be seen that the values of waiting time in the execution of some activities is too high. This can be explained by the following: 1) the process participants were inactive for some steps in the process; 2) the model did not fully account for the specifics of the employment of non-essential personnel. The assumption that non-essential staff use about 20% of their working time for planning activities implies that the waiting time for these staff is presumably used to perform activities related to their other job duties.

The process could also be improved with a cost change by making the following changes:

In one of the tabular reports of the study, it is shown that for a large part of the stages, more than 70% of the total time is used for waiting. In this respect, process improvements can be made through changes in the teams involved in planning activities in the Ministry of Defence, the Bulgarian Army and the structures subordinate to the Minister of Defence. In these teams, where possible, the same staff may be involved for several tasks. This practice is not new, but is currently applied on a limited basis.

4. *Improving the process by increasing resources.*
The application of this approach may be associated with:

- Eliminating some of the activities in the process.
- Introducing new technologies to reduce the cost and/or speed of completing each stage of the process.
- Changing the rules governing the process.
- Improving the process by acquiring new capabilities from the participants.

5. *Objective refinement of the model*
In order to achieve the set objective, it is necessary to reduce the value of the standard deviation. The standard deviation of the whole process is a function of the standard deviations of each stage. Using the process time table, it can be seen that certain stages affect the standard deviation the most. In order to reduce the overall value of standard deviation, the possibilities of reducing the deviation for these stages should be considered.

6. Additional recommendations by the analysis:

- Personnel costs are greatest for the implementation of “A22 Determination of Required Capabilities”. Additional measures are needed to reduce these costs.
- A lack of analytical tools and information technology to support system operations has been documented. This makes the interaction and exchange of information between organisational units and the work of officials and non-official bodies difficult. There is a need to compensate for the lack of real-time monitoring by management decision-makers, for example, by setting up an appropriate information system.
- There are tendencies to ignore risk as an element of governance, which reduces the quality and effectiveness of the functioning of the system. A clear risk management policy needs to be formulated.

IV. CONCLUSION

In accordance with the objectives, the following major contributions were obtained by the author:

1. A methodological toolkit with application of quantitative methods and simulation tools with proven usefulness in practice is proposed.
2. The processes of the current capability-based defence planning system are defined and documented.
3. A generalized research objective function (1) is defined. An analytical expression for finding the overall effectiveness of the system is presented.
4. The outcome indicators and their units of measurement are defined. These are used as measurement criteria.
5. Critical success factors have been identified through rank correlation.
6. An architecture of the current BA defence planning system has been developed.

7. A verification of the model's controllability with respect to the selected factors is made.

8. The formed activity model is checked for adequacy, consistency and completeness.

9. The performance of the system is simulated using specialized software tools.

10. The effectiveness of the system is evaluated.

11. Conclusions from the analysis are drawn. The conclusions are formulated on the basis of the results of the model analysis and are aimed at identifying opportunities for its improvement.

Exploring options to address the defined C2 performance issues is aimed at developing a future, improved system model and its implementation to address existing weaknesses.

In this paper, only Stage 1 of the proposed methodology for modeling and analyzing complex organizational systems is demonstrated. Following the recommendations from the analysis, according to the presented research methodology, a model of the desired state (To-Be) of the system still needs to be formed. It is an advanced model of the presented (As-Is) defence planning system. The perceived weaknesses in the (To-Be) model should be corrected. This can be done through a series of events, including the insertion or elimination of activities, the incorporation of analytical tools and new information technologies, and the reduction of supporting processes in the system. The model of the future state formed, similar to the (As-Is) model, shall be checked for adequacy, consistency, and completeness. Its efficiency shall be found. Using the described mathematical apparatus, the performance evaluation of the (To-Be) model shall be determined. A comparative analysis shall be made with the (As-Is) model to find the 'value added' after the changes made. In this way, all the activities identified in Step 2 of the methodology are performed.

In Stage 3, the programming implementation of a planning information system shall be presented. The stage should cover all activities and process actors. This includes: 1) the logical data model; 2) the descriptions of the system interfaces; 3) the description of the system communication tools; 4) the description of the system functionality; 5) the profile of the technical standards; 6) the programming sources as well as other specifics of the information system.

The study demonstrates the capabilities of an approach for evaluating alternatives to C2 systems. The approach generally involves modelling, analysis, and selection of advanced process solutions within a Defence Planning System. The results are the basis for activities to create an effective C2 system. The proposed approach has demonstrated applicability to all areas of management where capabilities and resources are involved.

ACKNOWLEDGEMENTS

The document was developed under the National Scientific Programme "Security and Defence", funded by the Ministry of Education and Science of the Republic of Bulgaria in implementation of the National Strategy for the Development of Scientific Research 2017-2030, adopted by Decision of the Council of Ministers No. 731 of 21 October 2021.

REFERENCES

[1] A. Lazarov, I. Radulov, and P. Andreeva P, Organisational-architectural modelling and transformational processes in defence, Military Journal, issue 6, Sofia, 2009, pp. 25-33, ISBN 0861-7392.

[2] J. Schekkerman, The Economic Benefits of Enterprise Architecture, Trafford Publ, 2005, ISBN 1-4120-6729-4.

[3] J. A. Zachman, A framework for information systems architecture, IBM Systems Journal, vol. 26, no 3, Reprint vol. 38, NOS 3&3, 1999, pp. 454-470.

[4] Architecture Capability Team Consultation, Command & Control Board, NATO ARCHITECTURE FRAMEWORK, Version 4, January 2018 Document Version 2020.07, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/9/pdf/NAFv4_2020.07.pdf, [Accessed: April. 07, 2024].

[5] E. Bozhinov and I. Vuchkov, Statistical methods for modelling or optimization of multifactorial objects: DI Technika, Sofia, 1973, UDC 519.2:62-52.

[6] Y. Yanakiev, T. Georgieva and T. Grozdanova, Methodology for assessing the organizational climate in the formations and structures of the Armed Forces of the Republic of Bulgaria: published by Military Academy "G. C. Rakovski", 2019, ISBN 978-619-7478-27-3.

[7] I. Radulov, Modelling of capability-based defence planning processes, National Scientific Program "Security and Defense", RTA 15th International Scientific and Practical Conference "ENVIRONMENT. TECHNOLOGY. RESOURCES", June 27-28, 2024, Vol. 4 (2024) page 218-223, https://journals.rta.lv/index.php/ETR/article/view/8214/6524 [Accessed: April. 07, 2024].

[8] Z. Zdravkov, E-network model for session protection in distributed relational databases, "Scientific Session 2001" with International Participation", Shumen 2001, ISBN 954-9681, pp. 212-219.

[9] R. S. Kaplan, S. Robert and R. Cooper, Process Costing as a Management Instrument, Frankfurt/Main, 1999.

[10] F. Melese, J. Blandin and S. O'Keefe, A New Management Model for Government: Integrating Activity-Based Costing, the Balanced Scorecard and Total Quality Management, The International Public Management Review 5:2, 2004: 103-30.

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 247-253

Implementing the Capabilities of the ATLAS Network to Improve the European Union's Counter-Terrorism Efforts

Raphael Röttinger
Vasil Levski
National Military University
Security and Defense Faculty
Veliko Tarnovo, Bulgaria
r.roettinger@aol.com

***Abstract*—The ATLAS Network was established by law enforcement special intervention units of the EU Member States and associated countries. All units who are part of this network are ready to respond to critical events and situations at any time when European security is at risk. The network is based at the Europol headquarters within the European Counter Terrorism Centre since 2018. It is continuously supported internally and directly connected to other networks in the law enforcement sector as well as other EU agencies. The subject of this study is the security of the European Union. The aim of this study is to reveal the possibilities for using the capabilities of the Atlas network to improve the security of the European Union. Based on the analyses conducted, some conclusions are drawn at the end of the article.**

Keywords*— *ATLAS, ATLAS Network, European Security, Counter Terrorism.

I. INTRODUCTION

Terrorism remains one of the most persistent security threats in the European Union (EU), evolving dynamically in response to political, economic, and technological changes [1]. The ATLAS Network, a collaborative initiative among elite special intervention units, plays an important role in enhancing the EU's counter-terrorism capabilities. This study examines the operational effectiveness of ATLAS, assessing its strengths and areas for improvement in responding to modern terrorist threats. A review of existing literature reveals differing perspectives on the role of multinational security cooperation in combating terrorism. While some sources emphasize the benefits of shared intelligence and joint training programs in enhancing rapid response capabilities, others highlight structural and legal limitations that hinder seamless cooperation between national security agencies. By integrating these insights, this research aims to evaluate the ATLAS Network's contributions to EU security and to propose recommendations for optimizing its operations to address emerging threats more effectively.

The literature on counter-terrorism efforts in the European Union presents a range of perspectives on the role and effectiveness of multinational security cooperation. Some studies, such as those by Aalberts and Werner (2011), emphasize the legal and institutional frameworks that shape cross-border counter-terrorism collaborations. They argue that regulatory inconsistencies between EU member states pose challenges for unified action. In contrast, Adamos et al. (2023) focus on the operational and technical dimensions of counter-terrorism, particularly the necessity of cybersecurity measures in combating digital threats. Other sources, including Turégano-Fuentes et al. (2008), provide case-based analyses of past terrorist attacks, shedding light on the response capabilities of law enforcement agencies and highlighting key areas for improvement. Europol reports (2023) and Lippay (2021) offer official insights into the ATLAS Network's role, detailing its structure, mission, and operational successes while also acknowledging gaps in interoperability and coordination. Scholars such as Bogain (2020) and Baker-Beall (2019) explore the sociopolitical context of counter-terrorism and discuss the implications of public discourse and securitization on policy-making.

This study synthesizes these varied perspectives to present a comprehensive evaluation of the ATLAS Network, balancing theoretical, legal, and operational considerations to assess its effectiveness in strengthening EU security.

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8499
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

A. Actuality of the Research

The increase in cross-border threats, lone-wolf attacks, and the use of modern technologies by terrorist groups necessitates a coordinated response among EU member states.

The variety of forms of terrorism, its asymmetric methods and means show many similarities with the features of contemporary low-intensity military conflicts. This makes the commitment and applicability of the combat capabilities of tactical formations a key attribute to achieve decisive and guaranteed results in the course of counterterrorism and counterterrorism activities. The breadth of the spectrum of applicability of modern tactical formations, albeit as a last resort, is justified by their potential capabilities for defensive and offensive countering of most forms of terrorism, which in addition to the capabilities of the forces for the preservation of internal state order, become a complex and adequate state and global response to new threats [2].

Terrorist structures are a new type of asymmetric adversary, having (in most of their forms of organization) an evolving, militarized and network-centric organization with a high degree of autonomy, discipline, determination and ideological conviction of their members, making it a threat equivalent to low-intensity warfare for the armed forces of EU states. The forms of tactical actions applied by terrorist field cells and the rapidly growing scale of conflicts caused by them justify the frequent counteraction of EU states with the help of army tactical formations. The broad spectrum of terrorist tactics and weapons, their gradual expansion from isolated acts to the setting of intra-state military conflict, and the magnitude of physical and psychological impact they achieve, define as possible and adequate the use of a large part of the combat capabilities of the army tactical formations for counter-terrorist and anti-terrorist actions.

The **ATLAS Network**, established as a specialized cooperation platform among elite counter-terrorism units, plays a crucial role in addressing these challenges [3]. Understanding the effectiveness and limitations of this network is essential to optimizing its contributions to EU security. It stands to reason that counter-terrorism will remain a priority for Europol and the EU, which means continuous improvement of the ATLAS Network and its modus operandi are of great importance. There needs to be close cooperation with all European partners to mitigate terrorist threats to the community by depriving terrorists of the means to limit their space to plan, finance and carry out attacks, by effectively countering radicalization and by strengthening information sharing and police cooperation [4].

B. Research Object

The object of this research is the **ATLAS Network**, its structure, functions, and its role in enhancing EU counter-terrorism capabilities through cooperation and coordination. One of the main focal point are the joint exercises and training programs within the network.

C. Research Goal

The primary goal of this research is to analyze the effectiveness of the ATLAS Network in strengthening counter-terrorism efforts in the EU and to explore potential improvements in its coordination and operational effectiveness.

To achieve this, the following assumptions for an optimal coaction of ATLAS have to be checked:

- There is a sufficient legal framework addressing all possible means of international law enforcement special operations and providing Europol as well as the ATLAS members with clearly lined out rules of engagement.
- Common protocols, stand-by routines, notice to move time, and constant and special responsibilities have to be established on the international (European) level.
- Common command structures at the scene or during the mission have to be institutionalized in order to bypass the requirement of adaption to local command structures.
- The compatibility of equipment and tactics has to be assured in order to allow for interoperability for teams of different nations.

If the institutions of the ATLAS Network prove to be less than ideal in these aspects, recommendations for improvement are developed.

D. Research Tasks

- Examine the current security landscape of the EU and the role of the ATLAS Network within this framework.
- Assess the coordination mechanisms within the ATLAS Network and propose enhancements for better security integration.
- Analyze past counter-terrorism case studies and ATLAS operations to identify strengths and weaknesses.
- Develop an improved concept for the joint training and education of ATLAS forces.

II. Materials and Methods

The research utilizes a **qualitative analysis** based on legal frameworks, case studies, and official reports from EU security agencies. Additionally, a **comparative approach** is applied to evaluate ATLAS' effectiveness relative to other counter-terrorism cooperation models.

The primary goal of this research is to analyze the effectiveness of the ATLAS Network in strengthening counter-terrorism efforts in the EU and to explore potential improvements in its coordination and operational effectiveness. To achieve this, the study employs a case study approach, examining contemporary terrorist attacks against EU member states in the 21st century. These case studies offer valuable insights into the operational

challenges and successes of counter-terrorism efforts, as well as the role of the ATLAS Network in crisis response.

Additionally, a survey amongst ATLAS members is conducted to gain knowledge about areas of improvement for joint ATLAS training and exercises.

A. Case Selection

Case studies provide a focused analysis of specific incidents, highlighting key operational responses, security gaps, and post-attack policy adaptations. However, their limited generalizability necessitates a comparative approach, ensuring that findings contribute to broader strategic recommendations. The cases selected represent diverse terrorist attack typologies, from large-scale coordinated attacks to cyberterrorism and chemical or biological threats, reflecting the evolving nature of terrorism in Europe.

B. Case Studies and Their Relevance

The Madrid train bombings in 2004 illustrate the challenges of coordinating emergency response efforts across multiple attack sites. The emergency medical response and evacuation were highly effective, but a lack of a unified command structure and inconsistent communication protocols created obstacles. In response, enhanced intelligence-sharing measures were introduced, and counter-terrorism cooperation within the EU intensified, underscoring the necessity of a standardized emergency response framework across member states [5].

The Paris Bataclan attacks in 2015 revealed the complexities of simultaneous terrorist actions targeting multiple locations. While special forces mobilized rapidly and emergency response mechanisms were activated, delays in intelligence coordination and response time were evident. The attack led to a review of cross-border intelligence sharing and operational coordination among EU law enforcement agencies [6].

The Berlin Christmas market attack in 2016 highlighted the difficulties in tracking radicalized individuals acting independently. Although the police response was quick and the attacker was identified, failures in preemptive surveillance and risk assessment were evident. As a result, improved surveillance measures and risk assessment frameworks were introduced, alongside physical security barriers at public events [7].

A similar attack occurred in Nice, France, in 2016, when a perpetrator used a truck to target a large crowd. This method of attack presented unique challenges, as conventional counter-terrorism strategies were not equipped to prevent vehicular attacks. The rapid medical response and immediate threat neutralization were commendable, but the incident demonstrated the need for urban security measures such as reinforced pedestrian barriers and vehicular restrictions in high-risk areas [8].

The Brussels airport bombing in 2016 underscored the threat posed by returning foreign fighters. The swift lockdown procedures and emergency response were effective; however, intelligence failures in tracking radicalized individuals proved detrimental. This event contributed to stronger international cooperation in monitoring and prosecuting individuals linked to foreign terrorist organizations [9].

The Manchester Arena bombing in 2017, the NotPetya cyberattack in 2017, the Salisbury Novichok poisoning in 2018, and the Cologne ricin attack attempt in 2018 are also selected as case studies.

These case studies provide critical insights into the effectiveness of EU counter-terrorism measures and the role of the ATLAS Network in responding to evolving threats. By analyzing past incidents, this research identifies areas for improvement, particularly in intelligence coordination, emergency response, and policy adaptation. The findings contribute to recommendations for enhancing the operational effectiveness of the ATLAS Network and ensuring a robust counter-terrorism framework in the European Union.

C. Research Limitations

- Access to classified operational data is restricted.
- The ATLAS Network is unique, limiting direct comparison with non-EU models.

The European Union's security architecture has evolved significantly in response to emerging threats and changing geopolitical dynamics. This analysis examines the current state of EU security, focusing on its legal framework, common security aspects, and persistent challenges in implementation.

D. Legal Framework of EU Security

The EU's counter-terrorism strategy is built on several key legislative and policy documents, including:

- EU Counter-Terrorism Strategy (2005, revised 2020)
- Directive (EU) 2017/541 on combating terrorism
- Europol's Counter-Terrorism Centre (ECTC)

The EU Counter-Terrorism Strategy, initially established in 2005 and revised in 2020, serves as the cornerstone of the Union's security approach. This foundational document is complemented by Directive (EU) 2017/541, which established comprehensive standards for combating terrorism across member states. The operational dimension is strengthened by Europol's Counter-Terrorism Centre (ECTC), which facilitates intelligence sharing and coordinates cross-border operations [10]. These frameworks aim to standardize security cooperation across member states, fostering intelligence sharing, operational coordination, and rapid response mechanisms.

E. Common EU Security Aspects

The EU's security strategy employs a four-pillar approach to counter-terrorism. The prevention pillar focuses on addressing root causes of radicalization and disrupting terrorist financing networks. The protection element emphasizes safeguarding critical infrastructure and

potential targets. The pursuit component strengthens law enforcement capabilities and cross-border cooperation. Finally, the response pillar ensures coordinated crisis management when incidents occur [11].

F. Current EU Security State

Despite robust frameworks and initiatives, the EU faces several significant security challenges. The persistence of fragmented national responses remains a primary concern, as member states maintain varying legal systems and operational procedures that can impede unified action. The digital age has introduced new vulnerabilities, particularly in the form of cyber (see NotPetya cyberattack in 2017) and hybrid threats, with online radicalization emerging as a significant concern [2]. Furthermore, coordination inefficiencies continue to hamper effective cross-border intelligence sharing, potentially creating security gaps that could be exploited by malicious actors.

It is evident that larger countries such as Spain, France, Italy and Germany experience more attacks and show higher arrest rates [12]. Looking forward, the EU's security framework must evolve to address these challenges while maintaining the delicate balance between security imperatives and fundamental rights. Enhanced integration of national security apparatuses, improved digital resilience, and streamlined intelligence-sharing mechanisms will be crucial for strengthening the EU's security posture [13].

The success of the EU's security strategy ultimately depends on member states' willingness to deepen cooperation and harmonize their approaches while maintaining the flexibility to address unique national security concerns [14], [15]. As threats continue to evolve, the EU's security framework must similarly adapt, ensuring robust protection for its citizens while preserving the values and freedoms that define the European project.

III. Results and Discussion

A. The ATLAS Network

1) Foundation of the ATLAS Network

The ATLAS Network was established in 2001 under the umbrella of **Europol** as a cooperative structure linking the special intervention units of EU member states. It was created to strengthen cross-border collaboration in counter-terrorism and high-risk law enforcement operations. Europol characterizes the ATLAS network in the following manner: 'The ATLAS network is comprised of specialized intervention units from the law enforcement agencies of the EU Member States and affiliated nations' [14].

All entities integrated within this network are equipped and prepared to address critical incidents and circumstances at any moment when the security of Europe is compromised. Since 2018, the network has been situated at Europol's headquarters within the European Counter-Terrorism Centre. It is perpetually sustained internally and is directly interconnected with other networks in the law enforcement domain as well as with various EU institutions. The network receives financial backing from Europol, facilitating the execution of several annual training exercises. A total of 38 specialized units are affiliated with the ATLAS network, encompassing units from non-EU countries such as Iceland, Norway, Switzerland, and two units from the United Kingdom [14].

2) Main Mission and Capabilities

The network's primary mission centers on enhancing the collective counter-terrorism capabilities of EU nations through three key mechanisms. First, it facilitates comprehensive joint training and simulation exercises, allowing units to develop common operational procedures and tactical understanding. Second, it maintains rapid response mechanisms that enable swift cross-border deployment during crises. Third, it serves as a platform for technological and tactical knowledge exchange, ensuring that best practices and innovative approaches are shared across all member units [16].

3) ATLAS Network Counter-Terrorism Units

ATLAS encompasses elite counter-terrorism units from all 27 EU member states, supplemented by observer participation from Norway, Switzerland, and the United Kingdom. Each member unit brings distinct specializations to the network [16]. Notable units include:

- GSG 9 (Germany) – Germany's GSG 9 has established itself as a leader in hostage rescue operations.
- RAID (France) – France's RAID unit excels in urban counter-terrorism scenarios.
- NOCS (Italy) Italy's NOCS specializes in high-risk arrests.
- UEI (Spain) – Spain's UEI has developed particular expertise in armed intervention and crisis response.
- SOBT (Bulgaria) – Bulgaria’s SOBT specializes in direct confrontation of organizational crime.

4) Key Characteristics

The network's effectiveness stems from its unique organizational characteristics. Its decentralized structure allows for flexible response capabilities while maintaining coordinated training programs across all member units. Each unit retains legal autonomy within its national framework, ensuring compliance with domestic laws while participating in international operations. This balance between independence and coordination is further enhanced by operational specialization, with different units developing expertise in specific counter-terrorism scenarios.

The ATLAS Network exemplifies the EU's commitment to sophisticated security cooperation while respecting national sovereignty. Its continued evolution and adaptation to emerging threats make it an essential component of Europe's counter-terrorism architecture. The network's success in combining operational effectiveness with respect for national autonomy provides a model for international security cooperation in an increasingly complex threat environment.

B. ATLAS Network and EU Security

The integration of the ATLAS Network into the European Union's security framework represents a significant advancement in transnational counter-terrorism capabilities. This analysis examines the network's current contributions to EU security and explores potential avenues for enhanced implementation.

1) Current Contribution to EU Security

ATLAS has significantly improved interoperability among special intervention units. The ATLAS Network has fundamentally transformed the landscape of special intervention unit cooperation across Europe. Its primary achievement lies in significantly improving interoperability among national counter-terrorism forces. This enhancement manifests in three critical areas: operational readiness, intelligence coordination, and procedural standardization [16].

The network's platform facilitates rapid cross-border deployment of specialized forces, addressing the crucial need for swift response capabilities in crisis situations. This operational readiness is complemented by sophisticated intelligence coordination mechanisms, enabling real-time information exchange through Europol's established channels. Furthermore, the standardization of operational tactics and crisis management protocols has created a common operational language among diverse national units, enabling more effective joint responses to security threats.

2) Possibilities for Better Implementation

Despite its successes, the ATLAS Network's potential for contributing to EU security could be further realized through several strategic improvements. Legal harmonization among EU member states represents a critical area for development. Greater alignment of counter-terrorism laws would facilitate more seamless cross-border interventions, reducing procedural delays in time-sensitive operations.

The establishment of a dedicated ATLAS Coordination Center could significantly improve strategic oversight and operational efficiency. Such a centralized command structure would enhance decision-making processes and resource allocation while maintaining the network's inherent flexibility.

In response to evolving threat landscapes, strengthening cyber-terrorism response capabilities within ATLAS has become increasingly crucial. This involves developing specialized teams equipped to address digital threats and cyber-attacks, which often transcend traditional national boundaries.

Enhanced civil-military cooperation presents another avenue for improvement. Closer integration with NATO and FRONTEX could create more comprehensive security operations, combining military expertise with law enforcement capabilities. This multi-dimensional approach would be particularly valuable in addressing hybrid threats that blur the lines between military and civilian security challenges.

3) Future Implications and Strategic Considerations

The potential enhancements to the ATLAS Network must be considered within the broader context of EU security evolution. Legal harmonization efforts need to balance operational efficiency with national sovereignty concerns. The development of a centralized command structure must maintain the network's existing strengths in decentralized operations while improving coordination capabilities.

The success of these improvements will largely depend on member states' willingness to deepen integration and share resources. Additionally, enhanced cooperation with other security organizations must be carefully structured to maintain clear operational boundaries while maximizing synergistic benefits.

As the European security landscape continues to evolve, the ATLAS Network's ability to adapt and enhance its capabilities will be crucial. The proposed improvements represent significant steps toward a more robust and responsive European security architecture, capable of addressing both current and emerging threats to EU security.

The ATLAS Network's evolution exemplifies the ongoing development of European security cooperation. By implementing these enhancements while maintaining its core strengths, the network can continue to serve as a crucial component in ensuring European security and stability.

4) Proposing a new and improved training program

The proposed new ATLAS training program builds upon the existing structures while introducing key enhancements to modernize and streamline training across EU special units. By addressing inconsistencies in training standards, incorporating digital learning, and refining practical exercises, the program ensures a more cohesive and effective operational framework.

A major improvement is the standardization of training content, ensuring that all ATLAS members, regardless of their national backgrounds, receive uniform instruction. This includes standardized tactical and operational procedures, unified communication protocols, and common first-aid techniques. By eliminating discrepancies, the program enhances coordination and cooperation in real-world missions.

The integration of a centralized learning management system (LMS) marks a significant step forward. This digital platform provides theoretical coursework, interactive tasks, and self-assessment tools, along with on-demand access to learning materials.

Additionally, it fosters peer learning, enabling participants to collaborate, discuss tactics, and share knowledge. This approach enhances flexibility, allowing

units to stay up to date without requiring constant in-person training.

Practical training remains at the core of ATLAS education, but the new framework refines it into two distinct categories. Non-critical operational exercises allow participants to experiment with tactical approaches in a low-risk environment, fostering adaptability. Meanwhile, critical operational exercises involve high-stakes scenarios, such as hostage rescues or counterterrorism operations, where expert trainers assess performance. This structured approach ensures that participants refine their decision-making and teamwork under both controlled and high-pressure conditions.

Another significant focus of the program is resilience and psychological readiness. Counterterrorism operations often involve extreme stress, making mental resilience essential. Training now incorporates psychological resilience coursework, simulated high-stress scenarios, and ongoing mental health support. By prioritizing psychological preparedness, the program aims to reduce burnout and enhance long-term operational effectiveness.

A structured evaluation system has also been introduced to maintain high training standards. Regular theoretical assessments through the LMS, performance evaluations after practical exercises, and peer feedback ensure that all trainees meet standardized competency levels before advancing to more complex modules.

To optimize resource allocation, the program retains existing Centers of Excellence (CoE) while implementing a structured mobility system for trainers and trainees. Instead of establishing new training centers, personnel will rotate between existing locations in Italy, Germany, Bulgaria, Hungary, and Slovakia. This strategy ensures even distribution of expertise while reducing logistical costs.

Strengthening international collaboration is another key focus. The program promotes regular multinational training exercises, real-time information exchange via SIENA, and joint tactical simulations between different national units. These measures enhance interoperability, allowing ATLAS forces to function as a cohesive entity in cross-border operations.

In total, the new ATLAS training program represents a comprehensive enhancement of existing structures. By combining standardization, digital learning, and advanced practical exercises, it strengthens European counterterrorism capabilities. Retaining core elements such as expert groups, CoE facilities, and multinational drills, while introducing harmonized training methods and resilience training, the program ensures a more efficient, adaptable, and cooperative special forces network. This initiative not only refines tactical skills but also fosters stronger international collaboration, making ATLAS an even more effective tool in safeguarding European security against evolving threats.

IV. Conclusions

1. Was the first research task successfully completed?

Yes. The study provided a comprehensive overview of the current EU security condition, highlighting the legal frameworks, common security aspects, and existing gaps.

2. Was the second research task successfully completed?

Yes. The research analyzed the ATLAS Network's effectiveness, its structural and operational components, and identified areas for improvement.

3. Was the research goal fully achieved?

Largely, yes. The research **confirmed the ATLAS Network's importance** in EU counter-terrorism efforts and provided **actionable recommendations** to improve its coordination and integration.

This study has provided a comprehensive analysis of the ATLAS Network's role in strengthening the European Union's counter-terrorism capabilities. The research successfully examined the EU's current security landscape, assessed the ATLAS Network's effectiveness, and identified key areas for improvement. The findings contribute both theoretically and practically to the field of security studies and counter-terrorism policy.

The study enhances the theoretical understanding of transnational security cooperation by demonstrating how multinational networks like ATLAS contribute to counter-terrorism efforts. It underscores the importance of interoperability, legal harmonization, and intelligence-sharing in overcoming fragmented national responses. Additionally, this research contributes to discussions on security governance by highlighting the balance between national sovereignty and collective security within EU law enforcement structures.

From a policy and operational perspective, the study offers actionable recommendations for optimizing ATLAS operations. Key proposals include the establishment of a centralized ATLAS Coordination Center to improve decision-making, standardization of joint training programs to ensure uniform tactical preparedness, and enhanced cyber-terrorism response capabilities to counter emerging digital threats. Furthermore, the findings support the need for deeper legal harmonization across EU member states to facilitate seamless cross-border interventions.

Future studies should explore the effectiveness of specific ATLAS interventions through empirical analysis of operational data. Additionally, further research into the integration of artificial intelligence and digital surveillance technologies within ATLAS operations could provide insights into modernizing counter-terrorism strategies. Legal scholars should also examine the feasibility of creating a unified European counter-terrorism legal framework to streamline multinational operations.

By bridging theoretical insights with practical recommendations, this study contributes to a more

coordinated and resilient counter-terrorism framework within the European Union. Strengthening the ATLAS Network's capabilities will be critical in ensuring the EU's preparedness against evolving security threats while maintaining democratic accountability and adherence to human rights standards.

REFERENCES

[1] T. E. Aalberts and W. G. Werner, "Mobilizing uncertainty and the making of responsible sovereigns," Review of International Studies, vol. 37, no. 5, pp. 2183-2200, 2011. . [Online]. Available: Cambridge Core, https://www.cambridge.org/ [Accessed Feb. 20, 2025], https://doi.org/10.1017/S0260210511000398

[2] K. Adamos, L. Filippopoulos, G. Stergiopoulos, and D. Gritzalis, "A Survey on National Cyber Emergency Plans," European Conference on Cyber Warfare and Security, vol. 22, no. 1, pp. 1-8, 2023. [Online]. Available: ECCWS https://papers.academic-conferences.org/index.php/eccws/index [Accessed Feb. 20, 2025], https://doi.org/10.34190/eccws.22.1.1039

[3] J. Ahmad, "Serving the same interests: The Wood Green ricin plot, media-state-terror relations and the 'terrorism' dispositif," Media, War & Conflict, vol. 12, pp. 411 – 434, 2018. [Online]. Available: Sage, https://journals.sagepub.com/ [Accessed Feb. 22, 2025], https://doi.org/10.1177/1750635218810922

[4] C. Baker-Beall, "The threat of the 'returning foreign fighter': The securitization of EU migration and border control policy," Security Dialogue, vol. 50, no. 5, pp. 437-453, 2019. [Online]. Available: Jstor, https://www.jstor.org/ [Accessed Feb. 17, 2025], https://www.jstor.org/stable/26979702

[5] F. Turégano-Fuentes, D. Pérez-Díaz, M. Sanz-Sánchez, and J. Alonso, "Overall Assessment of the Response to Terrorist Bombings in Trains, Madrid, 11 March 2004," European Journal of Trauma and Emergency Surgery, vol. 34, pp. 433-441, 2008. [Online]. Available: Springer Nature, https://link.springer.com/ [Accessed Feb. 15, 2025], https://doi.org/10.1007/s00068-008-8805-2

[6] A. Bogain, "Understanding public constructions of counter-terrorism: an analysis of online comments during the state of emergency in France (2015-2017)," Critical Studies on Terrorism, vol. 13, no. 4, pp. 591-615, 2020. [Online]. Available: Taylor & Francis, https://www.tandfonline.com/ [Accessed Feb. 18, 2025], https://doi.org/10.1080/17539153.2020.1810976

[7] J. Borg-Barthet and C. Lyons, C., "The European Union Migration Crisis," Edinburgh Law Review, vol. 20, pp. 230-235, 2016. [Online]. Available: Taylor & Francis, https://www.tandfonline.com/ [Accessed Feb. 17, 2025], https://doi.org/10.3366/ELR.2016.0346

[8] J.-P. Bouchard, J.-P., "Profile of the perpetrator of the Nice terror attack that took place on 14th July 2016: A terrorist whose modus operandi may have been imitated in other European attacks," Annales Médico-psychologique, vol. 176, no. 6, pp. 607-612, 2018. [Online]. Available: Sciencedirect, https://www.sciencedirect.com/ [Accessed Feb. 17, 2025], https://doi.org/10.1016/j.amp.2018.04.002

[9] Beauthier, W. Van de Voorde, P. Lefevre, and J.-P. Beauthier, "Belgium experience in disaster victim identification applied in handling terrorist attack at Brussels Airport 2016," Forensic Sciences Research, vol. 5, no. 3, pp. 223-231, 2020. [Online]. Available: Oxford, https://academic.oup.com/ [Accessed Feb. 20, 2025], https://doi.org/10.1080/20961790.2020.1775932

[10] S. D'Amato, "From BR to ISIS. The Italian domestic and international response to terrorism," European Politics and Society, vol. 19, no. 4, pp. 416-434, 2018. https://doi.org/10.1080/23745118.2018.1447763

[11] L. Peric, "An Exploration of the EU's Counterterrorism Measures," A Case Study Examining Italy, X-X, 2018. [Online]. Available: Taylor & Francis, https://www.tandfonline.com/ [Accessed Feb. 17, 2025], https://doi.org/10.22215/etd/2018-12722

[12] Europol, "TE-SAT Zusammenfassung," Europol.europa.eu, 2023. [Online]. Available: Europol, https://www.europol.europa.eu/ [Accessed Feb. 20, 2025], https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024%20-%20Zusammenfassung%20-%20DE.pdf

[13] G. Christou, "The collective securitisation of cyberspace in the European Union," West European Politics, vol. 42, pp. 278-301, 2018. [Online]. Available: Taylor & Francis, https://www.tandfonline.com/ [Accessed Feb. 17, 2025], https://doi.org/10.1080/01402382.2018.1510195

[14] Europol, "ATLAS Network," Europol.europa.eu, April 2023. [Online]. Available: Europol, https://www.europol.europa.eu/ [Accessed Feb. 20, 2025], https://www.europol.europa.eu/partners-collaboration/atlas-network

[15] O. Zinchenko, "European regional system for combating cyberterrorism: political, institutional and legal mechanisms," Issues of Political Science, vol. 39, pp. 118-122, 2021. [Online]. Available: Karazin, https://periodicals.karazin.ua/ [Accessed Feb. 20, 2025], https://doi.org/10.26565/2220-8089-2021-39-15

[16] C. Lippay, Der Atlas Verbund. Edewecht, Germany: Stumpf und Kossendy, 2021.

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 255-263

Exploring the Potential of Artificial Intelligence to Predict Cyber Attacks: Creation, Evaluation and Comparative Analysis of Effective Models of Fine-Tuning, Random Forests, and Neural Networks

Miroslav Stefanov
Computer science department
ULSIT
Sofia, Bulgaria
m.stefanov@unibit.bg

Boyan Jekov
Computer science department
ULSIT
Sofia, Bulgaria
b.jekov@unibit.bg

Tito Titov
Computer science department
ULSIT
Sofia, Bulgaria
t.titov@unibit.bg

Andrian Stoilov
Computer science department
ULSIT
Sofia, Bulgaria
a.stoilov@unibit.bg

Kiril Nikolov
Computer science department
ULSIT
Sofia, Bulgaria
k.nikolov@unibit.bg

***Abstract*— This quantitative investigation focuses on the application of artificial intelligence (AI) models for predicting cyberattacks and detecting anomalies in network traffic, aiming to enhance cybersecurity defenses. With the increasing complexity of cyber threats, AI offers a promising solution to address these challenges by providing predictive and responsive capabilities. This study compares three AI models — Fine-Tuning, Random Forests, and TensorFlow — using datasets aggregated on daily, weekly, and monthly levels. The methodology includes advanced data preprocessing, statistical analysis, and evaluation metrics such as RMSE, R^2, Precision, Recall, and F1-Score. Random Forests demonstrated exceptional accuracy and reliability, achieving high R^2 values and minimal errors. Fine-Tuning showed strong predictive capabilities but required careful parameter tuning to maintain accuracy. TensorFlow proved to be a powerful tool but required optimization to improve precision and reduce false positives. These results highlight the importance of model selection and parameter tuning in AI-driven cybersecurity applications.**

Keywords*— *Anomaly Detection, Artificial Intelligence, Cyber Attack Prediction, Cybersecurity, Machine Learning Models

I. Introduction

In the digital age, cybersecurity has become critical due to the exponential increase in cyberattacks, threatening individuals, organizations, and global infrastructure [1]. The increasing complexity and frequency of threats often exceed the capabilities of conventional defense mechanisms. Artificial Intelligence (AI), with its predictive and analytical strengths, offers promising solutions to these challenges [2]. This study investigates the potential of AI methodologies, specifically focusing on Fine-Tuning, Random Forests, and TensorFlow, to predict and mitigate cyber threats through anomaly detection and threat prediction.

The integration of Artificial Intelligence (AI) into cybersecurity highlights the need for adaptive and intelligent solutions to manage the dynamic nature of cyber threats [2]. Among AI-driven models, Random Forests and TensorFlow have shown particular promise. For example, Quezada et al [3] employed Random Forests in a bot infection detection system leveraging DNS fingerprinting, demonstrating the model's efficiency and adaptability in real-time anomaly detection. TensorFlow and deep learning models, as reviewed by Do et al. [4], have proven

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8504
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

effective in phishing detection through innovative approaches like Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. However, these methods face challenges such as the need for extensive training data and optimization to improve accuracy and scalability.

Despite these advancements, gaps remain in addressing issues like data availability and computational costs. This study evaluates the strengths and limitations of Fine-Tuning, Random Forests, and TensorFlow, focusing on their adaptability to evolving cybersecurity threats.

AI models have demonstrated substantial success in cybersecurity applications, particularly in predictive analytics and anomaly detection. Lichy et al. [5] highlight that classical machine learning models like Random Forest often outperform deep learning models such as Convolutional Neural Networks (CNN) and Gated Recurrent Units (GRU) in contexts like classifying encrypted malware traffic. Random Forest's robustness in structured data and lower computational complexity make it highly effective for real-time cybersecurity applications. However, TensorFlow and deep learning models excel in unstructured data contexts but face challenges such as susceptibility to overfitting and high computational demands. These limitations underscore the importance of selecting appropriate models based on specific scenarios.

This study evaluates the strengths of Fine-Tuning, Random Forests, and TensorFlow, focusing on their adaptability to cybersecurity applications and their ability to address operational constraints effectively.

Extensive research on AI applications in cybersecurity has highlighted methods for anomaly detection, DDoS attack prevention, and phishing detection. However, there is a notable gap in comparative studies evaluating diverse AI models on aggregated and temporally segmented datasets [6]. This study addresses this gap by assessing the performance of Fine-Tuning, Random Forests, and TensorFlow.

Fine-Tuning adapts pre-trained models to specific tasks by retraining with new data, leveraging existing knowledge to reduce computational and data requirements [7]. Random Forests, an ensemble method, improves classification and regression accuracy by reducing tree correlation through "bagging" and random feature selection [8]. TensorFlow, an open-source machine learning library, enables the creation and training of neural networks for complex computational tasks [9]. These models are evaluated for their adaptability to varied temporal datasets and operational constraints.

II. Materials and Methods

The analytical process in this qualitative research utilized widely recognized tools in scientific research, including Jupyter Notebook and Python. Jupyter Notebook was employed for its interactivity and ability to facilitate detailed data analysis. For analyzing models like Fine-Tuning, Random Forests, and TensorFlow, Python libraries such as Pandas were used for efficient data manipulation, while Matplotlib and Seaborn enabled clear and intuitive graphical visualization [10]. Scikit-learn provided advanced statistical models and machine learning algorithms, which were crucial for evaluating these models [11].

This team ensured the reliability of the analysis by conducting metadata standardization and validation procedures to identify anomalies that could influence results. Statistical methods such as mean, median, mode, standard deviation, and extreme value calculations were applied to provide a comprehensive understanding of the data distribution, which was critical for assessing these models in cybersecurity contexts.

The research methodology outlines the structured approach used to investigate the effectiveness of various AI models in cybersecurity applications. By leveraging robust platforms like Python and Jupyter Notebook, the research integrates advanced libraries for statistical computations, visualization, and machine learning. The methodology emphasizes data preprocessing, consistent training and testing practices, and rigorous performance assessment to ensure reliable results.

The analytical process in this research is organized using tools and platforms widely applicable in scientific studies, including Jupyter Notebook and Python. Jupyter Notebook offers an interactive environment for detailed data analysis, enhancing the workflow for evaluating models such as Fine-Tuning, Random Forests, and TensorFlow. Python libraries like Pandas are utilized for efficient data manipulation, while Matplotlib and Seaborn enable clear and intuitive graphical visualizations [10]. Scikit-learn is employed to apply advanced statistical models and machine learning algorithms [11], ensuring a robust framework for analyzing the performance of these models in cybersecurity.

This research team carried out metadata standardization and validation procedures to ensure the reliability of the analytical process. These steps were crucial in identifying and addressing any anomalies or exceptions that could impact the evaluation of models such as Fine-Tuning, Random Forests, and TensorFlow. The statistical analysis involved calculations for central tendency and dispersion, including means, medians, modes, standard deviations, and extreme values. These metrics provided a comprehensive understanding of the data distribution, supporting a robust assessment of the models' performance in cybersecurity contexts.

Analyzing cyberattacks based on aggregated data from various time periods provides critical insights into trends and patterns, essential for enhancing cybersecurity strategies. This research utilized three main datasets—Monthly, Weekly, and Daily—each contributing valuable information for evaluating the effectiveness of Fine-Tuning, Random Forests, and TensorFlow. The datasets were derived from actual cyberattacks, collected through the implementation of a honeynet system across multiple municipalities in Bulgaria.

To ensure compliance with legislative requirements, all data were anonymized and used exclusively for research purposes. The honeynet system simulated cyberattacks, capturing detailed information on attack behaviors and trends. This foundational data enabled the analysis of these AI models, supporting the development of predictive tools and improving defense strategies in cybersecurity.

Cyberattack data was analyzed using daily, weekly, and monthly temporal breakdowns to identify patterns and trends at different levels of granularity. This segmentation supported the development of AI models like Fine-Tuning, Random Forests, and TensorFlow, enabling them to perform short-term anomaly detection, medium-term trend analysis, and long-term attack predictions. By aligning temporal resolutions with specific analytical objectives, the study provided a robust framework for understanding and mitigating cybersecurity threats.

The dataset for daily analysis spanned 200 days, during which 196,494,832 attacks were recorded from all IP addresses, including 25,251,071 originating from Bulgarian IPs. On average, each honeypot registered 17,863,166 attacks, with attacks from Bulgarian IPs comprising 12.86% of the total. This data enabled models like TensorFlow and Random Forests to identify patterns and trends in daily attacks, enhancing their ability to detect anomalies and predict future cyber threats effectively.

A. File: Weekly

The Weekly dataset spans 20 months, equivalent to approximately 87 weeks, and includes a total of 196,494,832 recorded attacks from all IP addresses. Of these, 25,251,071 attacks originated from Bulgarian IPs, accounting for 12.86% of the total. On average, 113,006 attacks from all IPs and 14,046 attacks from Bulgarian IPs were registered daily, with foreign attacks surpassing Bulgarian ones by a factor of 6.78. The models utilized periodic attack patterns to build prevention strategies and strengthen anomaly detection capabilities. By differentiating between attacks from foreign and Bulgarian IPs, these models developed more precise detection mechanisms for identifying internal and external threats effectively.

B. File: Months

The monthly dataset spans 10 months and includes a total of 352,376,021 recorded attacks from all IP addresses. Of these, 26,004,126 attacks originated from Bulgarian IPs, accounting for 7.38% of the total. On average, 35,237,602 attacks from all IPs and 2,600,413 attacks from Bulgarian IPs were logged daily, with 4,783 unique Bulgarian IP addresses identified during this period. By analyzing geographic characteristics and network topology, these models classified attack types and distinguished IP origins. This approach enabled the models to detect and predict large-scale patterns effectively, addressing both local and global cybersecurity threats.

All collected data were meticulously anonymized to adhere to legislative and ethical standards, ensuring the integrity of the research. The anonymization process involved removing or masking any personally identifiable information (PII) and sensitive metadata to eliminate privacy risks. These datasets were utilized exclusively for research purposes, enabling the evaluation of models, while safeguarding participants' privacy and fostering robust cybersecurity analysis.

C. Software Tools for Analysis

The analysis and evaluation of cyberattack data in this study required the use of advanced software tools to ensure accuracy and efficiency. Python served as the primary platform for implementing models like Fine-Tuning, Random Forests, and TensorFlow, supporting data manipulation, preprocessing, and machine learning tasks. Key libraries, including Pandas for data handling [12], Matplotlib and Seaborn for visualization [10], [13], and Scikit-learn for machine learning algorithms [11], provided robust analytical capabilities.

Jupyter Notebook offered an interactive environment that enhanced reproducibility and iterative experimentation, critical for refining these models' workflows [14]. These tools enabled the systematic analysis of cyberattack patterns and facilitated comprehensive evaluations of the models' predictive performance, contributing to advancements in cybersecurity applications.

Pandas was integral to the research process, supporting high-performance data manipulation and preprocessing for models. It was used to load and structure large datasets, including network traffic logs and metadata on cyberattacks, ensuring the data was well-organized for further analysis. The tool supported cleaning processes, such as removing missing values and duplicate entries, and normalized numerical features to ensure compatibility with machine learning algorithms. Furthermore, Pandas facilitated the splitting of data into training and testing subsets, essential for evaluating these models' performance. Its exploratory data analysis capabilities helped identify key trends and anomalies in the initial dataset, providing critical insights for building effective machine learning workflows [12].

Matplotlib and Seaborn were essential tools for visualizing data and interpreting results in the evaluation. Matplotlib was used to create scatterplots and boxplots, enabling the visualization of data distributions and the identification of potential outliers. Seaborn complemented these capabilities by generating heatmaps and KDE plots, which highlighted correlations and local trends among network traffic features. These visualizations were instrumental in guiding the selection of appropriate anomaly detection algorithms and in understanding the key outputs of these models. By providing clear graphical representations, Matplotlib and Seaborn enhanced the analytical process and supported informed decision-making throughout the research [10].

Scikit-learn was a central tool for implementing and evaluating the performance of AI models like Fine-Tuning, Random Forests, and TensorFlow. It enabled the

integration of advanced methods for anomaly detection and predictive analytics, ensuring seamless implementation and evaluation workflows. The library provided automated computation of key metrics such as Precision, Recall, F1-score, and RMSE, which were critical for assessing model performance. This comprehensive functionality made it indispensable for refining these models and enhancing their effectiveness in cybersecurity applications [11].

Jupyter Notebook was a central platform for executing, documenting, and visualizing the research process, particularly for thee models. Each stage of the analysis was organized into individual cells, enabling iterative testing and optimization of these models and their associated hypotheses. The interactive environment provided visual feedback through embedded graphs and tables, facilitating dynamic parameter tuning and improving the efficiency and clarity of the analysis [14].

D. Comparison of Methods

Three AI models Fine-Tuning, Random Forests and TensorFlow (neural networks), were selected for this study to evaluate their effectiveness in predicting cyberattacks and detecting anomalies in network traffic. The study was done in three steps. The first one was Training and Testing - Each model was trained and tested on the same datasets to ensure consistency in comparisons. The second one was Handling Model Specifics - Hyperparameter optimization was applied to neural networks, such as TensorFlow. And the last one was Performance Assessment - Each model's effectiveness was evaluated using key metrics (see the "Metrics section), which measure both predictive and classification performance.

Three primary datasets Days, Months, and Weekly, were utilized to provide varying temporal contexts for analyzing cyberattack patterns. Data preprocessing involved removing missing or duplicate values and normalizing or standardizing features where needed. For models like TensorFlow, the datasets were split into training, validation, and test subsets, ensuring robust evaluation and optimization.

The analysis goals varied for each dataset: daily data enabled time-series analysis to identify short-term trends, while monthly data offered a long-term perspective on global anomalies. Weekly data supported the discovery of periodic patterns and comparisons between internal (Bulgarian) and external (foreign) threats. This structured approach allowed TensorFlow, Random Forests, and Fine-Tuning to adapt to diverse cybersecurity challenges effectively.

The effectiveness of the models was evaluated using a range of metrics tailored to their functionalities. RMSE measured the average error, making it ideal for regression models like TensorFlow, while R^2 assessed the proportion of data variability explained by each model, indicating their predictive accuracy. Precision and Recall were used to evaluate classification tasks, focusing on the models' ability to identify cyberattacks and detect true positives accurately. F1-Score provided a harmonic mean of Precision and Recall for a balanced evaluation.

To ensure the robustness of the results, cross-validation was employed for all models, with repeated tests conducted on varied subsets. This approach minimized the risk of overfitting and improved the generalizability of Fine-Tuning, Random Forests, and TensorFlow. Consistent validation practices ensured reliable performance assessments for these models.

After applying each model to the datasets, the results were compared using the outlined metrics. Fine-Tuning demonstrated high accuracy but was sensitive to minor changes in the data. Random Forests showed perfect metrics, though results may indicate potential overfitting. TensorFlow showed that significant hyperparameter optimization is required for better results.

III. Results and Discussion

The following chapter focuses on the analysis and evaluation of AI models, including Fine-Tuning, Random Forests, and TensorFlow, applied to cybersecurity. The evaluation uses performance metrics five to measure the models' effectiveness in predicting cyberattacks and detecting anomalies. These analyses provide valuable insights into selecting and optimizing AI models based on specific cybersecurity objectives and data characteristics. The findings emphasize the importance of tailoring AI methodologies to align with real-world cybersecurity challenges, enhancing the models' effectiveness in anomaly detection and predictive defense strategies.

The Fine-Tuning Model demonstrates consistent predictive capabilities, as evidenced by the RMSE (Root Mean Square Error) value of 726,738.906. While this value indicates some deviations from actual data, it remains within reasonable limits for models applied to large and complex datasets. Performance metrics suggest that the model is suitable for applications requiring high accuracy in predictive tasks and analytical processing. The results presented in Table 1were achieved through a systematic testing and validation process that ensures the model's reliability. The methodology is detailed below:

The data was divided into training (80%) and testing (20%) subsets. The training set was used to build the model, while the testing set provided an independent assessment of the model's generalization capability.

During training, the k-fold cross-validation method was applied. This approach ensured consistent model performance across different data partitions and reduced the likelihood of overfitting. It also facilitated the optimization of hyperparameters.

Prior to training, the data was balanced to ensure equal representation of all classes. This step minimized biases in classification metrics, particularly precision and recall.

The model underwent hyperparameter tuning using methods such as grid search. This process aimed to minimize RMSE and improve classification metrics,

ensuring the model's reliability across different configurations.

Test RMSE: Calculated to quantify the average prediction error. This metric penalizes larger deviations more heavily, making it an effective indicator of predictive accuracy.

Test R^2: The coefficient of determination, with a value of 0.985, highlights the model's ability to explain data variation. This high R^2 value indicates that the model fits the data well.

Precision, Recall, and F1 Score: These metrics were calculated to evaluate the model's classification performance. Scores of 1.0 for all these metrics suggest that the model effectively distinguishes between classes without false positives or negatives.

Residual errors (differences between predicted and actual values) were analyzed to confirm their random distribution. This step validated the model's predictions and ensured the absence of systematic biases.

Results were validated on the independent test dataset (20%), which was not used during training or hyperparameter tuning. This ensured an unbiased evaluation of the model's performance.

TABLE 1 TABLE OF TEST RESULTS OF FINE-TUNING MODEL

Metric	***Value***
Test RMSE	726,738,906
Test R^2	0.985
Precision	1.0
Recall	1.0
F1 Score	1.0

By adhering to this testing and evaluation process, the model demonstrates its robustness. Future work could involve applying the model to more diverse datasets to confirm its generalization capabilities and enhance its predictive accuracy.

Although the RMSE value is relatively high, possibly due to the complexity of the data or the specifics of the study, the Fine-Tuning Model exhibits reliable performance in predictive and classification tasks. It is well-suited for applications requiring precision and detailed analytical capability. As such, this model becomes a valuable tool in the field of data analysis, particularly in the context of malware detection and network traffic anomaly detection, where accuracy and prediction reliability are key.

The results in Table 2 for the Random Forests model were achieved through a systematic testing process, which aimed to evaluate the model's performance comprehensively. See Table 2 for details. Below are the detailed steps of the methodology and considerations for interpreting the outcomes:

The dataset was divided into training and testing sets in an 80-20 split. The training set was used to build the model, while the test set was reserved for an unbiased evaluation of the model's performance.

The training set underwent k-fold cross-validation to enhance reliability. This step helps ensure that the model performs consistently across different subsets of the data and minimizes the risk of overfitting.

Grid search and random search techniques were applied to optimize key hyperparameters, such as the number of trees, maximum depth, and splitting criteria. These optimizations were aimed at maximizing predictive accuracy while preventing overfitting.

The dataset was checked and adjusted for class balance to prevent bias toward the majority class. Techniques such as oversampling the minority class or undersampling the majority class were applied where necessary.

Test RMSE: The Root Mean Square Error measures the average error magnitude between the predicted and actual values. An RMSE of 0.0 may suggest potential data or evaluation anomalies.

R^2 Score: A score of 1.0 reflects that the model explains 100% of the variance in the target variable, which aligns with the RMSE of 0.0.

Precision, Recall, and F1 Score: All these metrics recorded perfect values of 1.0, signifying flawless classification performance.

TABLE 2 TABLE OF TEST RESULTS OF RANDOM FORESTS

Metric	***Value***
Test RMSE	0.0
Test R^2	1.0
Precision	1.0
Recall	1.0
F1 Score	1.0

Residual Analysis:

The results presented in the table demonstrate the performance of the Random Forests model, with Precision, Recall, and F1 Score reaching values of 1.0. Additionally, RMSE is reported as 0.0, and R^2 has a value of 1.0. However, these results require further analysis to ensure their reliability and identify potential issues such as overfitting or data anomalies.

The model must be tested on an independent dataset that was not used during training or testing to validate the results. Conducting tests with more complex and diverse datasets is necessary to assess the model's ability to generalize to real-world data. As part of the analysis, it should be noted that the results reported in the table may indicate overfitting. This suggests that the model may be overly tailored to the training data and fail to generalize

effectively to new, unseen data, leading to unrealistic performance metrics.

The possibility of data leakage, where test data may have influenced the training process, must be considered. Additionally, an overly simplistic dataset could lead to exaggerated results, underscoring the need for using complex and realistic datasets. If the model bases its predictions on irrelevant or non-essential features, it could compromise its ability to perform effectively on new and unseen data.

Analyzing the importance of features is crucial to ensure that the model relies on relevant data rather than noise. The perfect results could also stem from statistical errors or anomalies in the testing process, which requires a thorough review of residual errors and key metrics.

Random Forests perform well in the analysis of large datasets with many features, demonstrating their capabilities in both classification and regression analysis. They can be used to classify days with high and low probability of attacks based on historical data.



Fig. 1. Graph: Comparison of true and predicted values from Random Forest

The Figure 1 graph shows a comparison between the true values (X-axis) and the predicted values (Y-axis) for daily cyber attacks. The dashed line represents the ideal correlation, where the predicted values perfectly match the true values. Most points are aligned close to this ideal line, indicating that the model successfully captures the overall trends in the dataset. However, the following two points show noticeable deviations, highlighting areas where the model's predictions differ from the actual data.

Mean Squared Error (MSE): MSE is approximately 31,992,930,846. This high value reflects the quadratic scale of deviations and is influenced by the large magnitude of the target variable (daily cyber attacks) and the inherent variability in the dataset. It is important to note that MSE is sensitive to outliers, which can further increase this value.

Root Mean Squared Error (RMSE): RMSE is 178.866, providing a more intuitive measure as it is in the same unit as the target variable. This value suggests a reasonable average deviation between the predicted and true values, considering the high variability of the cyber attack data.

The average number of attacks recorded per day is averaged based on the number of honeypots deployed in the investigated areas. This averaging of attacks per honeypot per day is crucial for providing an accurate and representative analysis. The reason for using this approach is to minimize the impact of differences in the number of active honeypots during the observation period and to ensure uniformity in the presented data.

Based on multiple decision trees, random forests incorporate randomness in the training of submodels to reduce the variance of predictions and improve overall predictive power.

In the context of cyber security, random forest models allow analysis of the interaction between different variables and their influence on the probability and intensity of cyber attacks. Thanks to their ability to combine hundreds or even thousands of individual decision trees, these models can provide deep insights into data characteristics and predict potential attacks with high accuracy.

When using random forests for regression tasks, the model shows robust results as measured by RMSE, which allows an accurate estimation of the mean prediction error. For classification tasks, the model can be evaluated with an F-score, which provides a balanced measure of the model's accuracy and responsiveness to different classes. However, the F-score must be calculated in the context of clearly defined classification criteria that meet the specific needs of the cybersecurity problem.

Random forests are proving to be a reliable and flexible tool for cybersecurity analysis and prediction. Their ability to process large data sets and identify complex patterns makes this approach valuable for developing effective defense strategies and preventing future attacks. Future research can focus on fine-tuning the model and exploring integration opportunities with other ensemble and machine-learning techniques to further increase predictive accuracy and address the dynamically changing challenges in cyberspace.

Deep Learning can detect complex non-linear relationships in data and predict future attacks, making it a powerful tool for modeling intricate relationships. Recurrent Neural Networks (RNNs) are particularly well-suited for time series and sequential data, allowing for various applications such as prediction, classification, regression, and even data generation. Neural networks are versatile and can be utilized for a wide range of tasks, including classification, regression, time series forecasting, and more. When the data exhibits complex non-linear relationships, deep learning approaches, particularly RNNs, can be effective for analyzing attack data. See Table 3 for metrics and values.

TensorFlow is an open source machine learning software library that provides tools for building and training neural networks to recognize and discover patterns and correlations in large data sets. This open source machine learning software library is suitable for a wide range of tasks including regression, classification, automatic text generation, image processing and many others. Neural networks are particularly powerful in

extracting complex features from data and are suitable for irregular data where relationships can be non-linear and complex. See Table 3 for details.

TABLE 3 TABLE OF TEST RESULTS OF TENSORFLOW

Metric	***Value***
Test RMSE	1,890,971,414
Test R^2	0.9018
Precision	0.0
Recall	0.0
F1 Score	0.0

On the graph, we see the distribution of predicted values versus true values. The dashed red line represents the perfect fit where the predicted values equal the true values. Dots represent actual model predictions; the closer they are to the red line, the more accurate the predictions.

Based on the RMSE and R^2 values you provided:

RMSE (Root Mean Squared Error): 1,890,971.414 - This is a relatively high value, which means that your predictions are significantly off the true values. Ideally, we want the RMSE to be as low as possible.

R^2 (Coefficient of Determination): 0.9018 - This is a fairly high value indicating that the model explains about 90% of the variation in the true values. However, the high value of RMSE indicates that despite the good fit of the data, the error variances are significant.

The graph shows that most of the predictions are close to the line of perfect fit, but there are some significant deviations.

This could be due to several factors:

The model may encounter challenges with certain 'outliers' or data points that significantly differ from the rest of the dataset. There could also be anomalies or extremely high or low values in the data that the model failed to predict accurately. Additionally, the dataset might lack sufficient diversity or contain hidden factors that the model was unable to capture.

In the context of regression, the Precision, Recall, and F-score metrics are not directly applicable, as they are defined for classification tasks. In regression, predictor values are continuous rather than discrete classes. However, if you want to convert the regression problem into a classification problem, you need to define a threshold where values above this threshold are considered one class (e.g. "attack") and values below it another (e.g. "not attack").

The TensorFlow model included in this analysis reveals significant challenges in its ability to make accurate and reliable predictions. With the highest RMSE (Root Mean Square Error) value of 1,890,971.414, this model has difficulties in accurately predicting the results, which is manifested in significant discrepancies between the predicted and actual values. A high RMSE value is an indicator of large prediction errors, which calls into question the reliability of the model in practical applications.

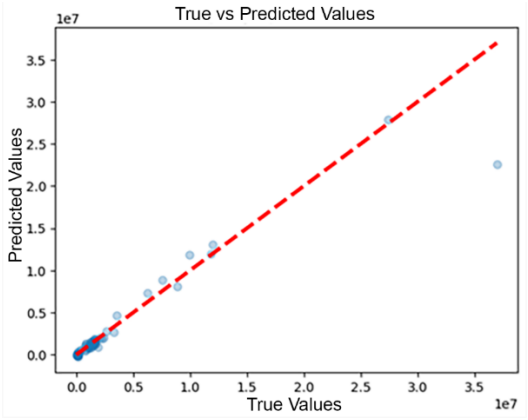


Fig. 2. Graph: Neural Networks - True versus predicted value

Furthermore, the R^2 value of 0.901, although relatively high, indicates that there is still a significant portion of the variation in the dependent variable that is not explained by the model. This suggests that the model may not include all relevant factors or interactions that are necessary for accurate prediction.

Most concerning are the zero Precision, Recall, and F-score values, which point to serious gaps in the model's ability to identify and classify relevant cases. This indicates that the model failed to correctly predict the positive cases, which is critical for tasks such as malware and network anomaly detection.

In conclusion, based on these results, the TensorFlow model requires significant improvements, including potentially retraining with more appropriate data or parameter tuning. It may also be necessary to investigate alternative models or techniques to achieve higher accuracy and reliability in predictions. At this stage, the model seems inadequate for the tasks at hand, especially in the context of cybersecurity and anomaly detection.

IV. CONCLUSIONS

In the context of regression, the Precision, Recall, and F-score metrics are not directly applicable, as they are defined for classification tasks. In regression, predictor values are continuous rather than discrete classes. However, if you want to convert the regression problem into a classification problem, you need to define a threshold where values above this threshold are considered one class (e.g. "attack") and values below it another (e.g. "not attack").

Table 4 contains the results of the different AI models:

TABLE 4 RESULTS OF THE AI MODELS

AI Model	*RMSE*	*R^2*	*Precision*	*Recall*	*F-score*
Fine Tuning Model	726,738,906	0.985	1.0	1.0	1.0
Random Forests	0.0	1.0	1.0	1.0	1.0
TensorFlow	1,890,971,414	0.901	0	0	0

*The ranking presents the models from highest to lowest performance on these metrics.

This table presents a comparative analysis of different AI models, including statistics such as root mean square error (RMSE), coefficient of determination (R^2), precision (Precision), range (Recall) and F-score, which allows evaluation of the effectiveness of each model.

The analysis of the results presented in the preceding table reveals significant differences in the performance of the different AI models in the context of the prediction or classification task within the studied data.

Fine Tuning Model: The Fine Tuning Model shows exceptional precision and stability as noted by the low RMSE value (726,738.906) and high coefficient of determination ($R^2 = 0.985$). This suggests that the model has an excellent ability to adapt to the data and generate accurate predictions.

Random Forests: The Random Forests model demonstrated a perfect score in all dimensions - RMSE (0.0), R^2 (1.0), Precision (1.0), Recall (1.0) and F-score (1.0). Such results may be indicative of an overtrained model, since a perfect result is rare in real-world applications.

TensorFlow: The TensorFlow model shows significant difficulty with an RMSE of 1,890,971.414 and an R^2 of 0.901, suggesting that the model may not be adequately trained or missing key features from the data.

In summary, the results emphasize the criticality of selecting a model that aligns with the characteristics of the data and the specific task requirements. While certain models demonstrate high precision and reliability, others may necessitate further tuning or refinement to enhance their predictive capabilities. Among the analyzed AI models, Random Forests stand out as the most effective, delivering exceptional accuracy and reliability across all evaluated metrics. With maximum Precision, Recall, and F-score values, alongside minimal RMSE and maximum R^2, Random Forests excel in both prediction and classification tasks, making them an optimal choice for applications demanding high accuracy. Conversely, the TensorFlow model faces notable limitations, rendering it less suitable for critical use cases that require stringent accuracy and reliability standards. Despite its widespread use, TensorFlow requires significant optimization and adjustments to match the performance levels of leading models like Random Forests.

Random Forests emerge as the optimal choice for complex analysis and prediction, demonstrating exceptional accuracy and reliability across diverse applications. This model consistently delivers robust and precise solutions for a broad range of tasks within machine learning and artificial intelligence. The analysis of the AI models highlights their effectiveness based on key criteria, including predictive accuracy (RMSE), the ability to explain data variability (R^2), and classification performance (Precision, Recall, and F-score). These findings reinforce Random Forests as a highly dependable tool for addressing complex computational challenges.

This research examined various machine learning models, emphasizing their predictive and classification capabilities. The Random Forests model demonstrated exceptional performance, achieving perfect metrics, including a zero RMSE and a maximum R^2 value of 1.0, underscoring its robustness and reliability. The Fine-Tuning model also performed well, with high R^2 values and near-perfect Precision, Recall, and F-score metrics, though its RMSE was higher compared to Random Forests. In contrast, the TensorFlow model exhibited notable limitations, with significant discrepancies in prediction accuracy and low or zero Precision, Recall, and F-score values, highlighting challenges in classification tasks. This analysis provides an in-depth exploration of the strengths and weaknesses of various machine learning approaches, reinforcing the importance of selecting models tailored to specific tasks and datasets.

REFERENCES

[1] "How AI will automate cybersecurity in the post-COVID world | VentureBeat." Accessed: Feb. 25, 2025. [Online]. Available: https://venturebeat.com/business/how-ai-will-automate-cybersecurity-in-the-post-covid-world/

[2] "Hands-On Artificial Intelligence for Cybersecurity | Data | Paperback." Accessed: Feb. 25, 2025. [Online]. Available: https://www.packtpub.com/en-us/product/hands-on-artificial-intelligence-for-cybersecurity-9781789804027

[3] V. Quezada, F. Astudillo-Salinas, L. Tello-Oquendo, and P. Bernal, "Real-time bot infection detection system using DNS fingerprinting and machine-learning," *Computer Networks*, vol. 228, p. 109725, Jun. 2023, doi: 10.1016/J.COMNET.2023.109725.

[4] N. Q. Do, A. Selamat, O. Krejcar, E. Herrera-Viedma, and H. Fujita, "Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions," *IEEE Access*, vol. 10, pp. 36429–36463, 2022, doi: 10.1109/ACCESS.2022.3151903.

[5] A. Lichy, O. Bader, R. Dubin, A. Dvir, and C. Hajaj, "When a RF beats a CNN and GRU, together—A comparison of deep learning and classical machine learning approaches for encrypted malware traffic classification," *Comput Secur*, vol. 124, p. 103000, Jan. 2023, doi: 10.1016/J.COSE.2022.103000.

[6] S. Aktar and A. Yasin Nur, "Towards DDoS attack detection using deep learning approach," *Comput Secur*, vol. 129, p. 103251, Jun. 2023, doi: 10.1016/J.COSE.2023.103251.

[7] J. Devlin, M.-W. Chang, K. Lee, K. T. Google, and A. I. Language, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," *Proceedings of the 2019 Conference of the North*, pp. 4171–4186, 2019, doi: 10.18653/V1/N19-1423.

[8] L. Breiman, "Random forests," *Mach Learn*, vol. 45, no. 1, pp. 5–32, Oct. 2001, doi: 10.1023/A:1010933404324/METRICS.

[9] M. Abadi *et al.*, "TensorFlow: Large-Scale Machine Learning on Heterogeneous Distributed Systems," Mar. 2016, Accessed: Feb. 25, 2025. [Online]. Available: https://arxiv.org/abs/1603.04467v2

[10] J. D. Hunter, "Matplotlib: A 2D graphics environment," *Comput Sci Eng*, vol. 9, no. 3, pp. 90–95, 2007, doi: 10.1109/MCSE.2007.55.

[11] F. Pedregosa FABIANPEDREGOSA *et al.*, "Scikit-learn: Machine Learning in Python," *Journal of Machine Learning Research*, vol. 12, no. 85, pp. 2825–2830, 2011, Accessed: Feb. 25, 2025. [Online]. Available: http://jmlr.org/papers/v12/pedregosa11a.html

[12] W. McKinney, "Data Structures for Statistical Computing in Python," *scipy*, pp. 56–61, 2010, doi: 10.25080/MAJORA-92BF1922-00A.

[13] M. L. Waskom, "seaborn: statistical data visualization," *J Open Source Softw*, vol. 6, no. 60, p. 3021, Apr. 2021, doi: 10.21105/JOSS.03021.

[14] T. Kluyver *et al.*, "Jupyter Notebooks – a publishing format for reproducible computational workflows," *Positioning and Power in Academic Publishing: Players, Agents and Agendas - Proceedings of the 20th International Conference on Electronic Publishing, ELPUB 2016*, pp. 87–90, 2016, doi: 10.3233/978-1-61499-649-1-87.

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 265-269

The Impact of Change Management on the Quality of the Work Environment: A Study of the Employer-Employee Relationship of Senior Customs Supervisors

Vladislavs Sardiko
Faculty of Education and Management
Daugavpils University
Daugavpils, Latvia
vl.sardiko@gmail.com

Dzintra Ilishko
Institute of Humanities and Social Sciences
Daugavpils University
Daugavpils, Latvia
dzintra.ilisko@du.lv

***Abstract*- This study examines the impact of change management on the quality of the work environment by analysing the employer-employee relationship among senior customs supervisors working at Latgale customs checkpoints. The necessity to adapt personnel management approaches within the Customs Board is highlighted, taking into account the sustainable development goals of the institution. A quantitative survey was conducted involving 113 respondents, representing different socio-demographic groups. The analysis of the results revealed significant differences in the perception of work environment dimensions, with educational level showing the strongest influence. However, gender, marital status, family responsibilities, and management experience also showed variations that should not be overlooked when shaping change management strategies. The findings demonstrate that socio-demographic and professional profiles have a complex effect on employees' satisfaction and perception of the working environment. Based on the results, recommendations are proposed to incorporate these factors systematically into personnel management practices, aiming to strengthen institutional efficiency and improve the well-being of customs employees.**

Keywords — Change management, Customs Board, senior customs supervisors, work environment

I. INTRODUCTION

The process of managing organizational change is essential for ensuring the sustainability and performance of institutions, particularly in the context of public administration [1], [2]. For organizations like the Customs Board, change management is not only about adjusting operations but also about fostering an environment where employees can contribute effectively to organizational development [3]. Senior customs supervisors, who play a crucial role at customs checkpoints, directly experience the effects of organizational changes, making their relationship with the employer critical for shaping a supportive work environment [4].

Understanding the impact of change management on the work environment is particularly important for the Customs Board [5]. This study focuses on the employer-employee relationship, with particular emphasis on senior customs supervisors working at Latgale customs checkpoints. By analyzing factors such as socio-demographic characteristics, education levels, and income sources, the research aims to formulate recommendations that will contribute to improving the quality of the work environment and enhancing overall institutional performance.

Change management in public administration is a complex process that affects both organizational structures and employee behavior. According to Kotter [1], successful organizational change requires effective leadership and communication strategies that align employee interests with organizational goals. In the customs sector, where regulations and operational procedures are constantly evolving, it is vital to support employees with clear leadership and the provision of necessary resources [6].

Further perspectives highlight that successful change processes also depend on organizational readiness and structured transition management. Lewin [7] introduced a three-phase model emphasizing the importance of preparing for change, guiding the transition, and reinforcing new behaviors. Armenakis and Harris [5] stressed that employee belief in the necessity and feasibility

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8497
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

of change initiatives is crucial for success. Hayes [8] similarly notes that both system-level interventions and the individual motivation of employees must be balanced during organizational changes.

Modern approaches also emphasize the importance of good governance principles and strategic human resource management within public institutions. The European Commission [9] and Hughes [10] argue that sustainable change in public organizations, including customs administrations, requires active employee involvement, transparent leadership, and structured adaptation processes.

These theoretical approaches collectively offer valuable insights for improving change management practices, particularly in environments such as the Customs Board, where both external regulations and internal employee dynamics must be effectively balanced.

II. Materials and Methods

This study uses a structured survey tool designed to capture the employer-employee relationship. A total of 38 questions, adapted specifically for senior customs supervisors, were administered using a Likert scale (ranging from 1 to 5, where 1 represents "Strongly Disagree" and 5 represents "Strongly Agree"). The survey aimed to assess various dimensions of the work environment, including work processes, job satisfaction, health, conflict resolution, and the impact of digitalization.

The survey data were analyzed to identify statistically significant differences between various socio-demographic groups. These groups included gender, family status, education level, and competency levels. The analysis utilized t-tests to determine whether differences in perceptions of the work environment existed between these groups.

III. Results and Discussion



Fig. 1. Dimensions of the work environment by gender

There are statistically significant differences in the perception of working conditions between women (3.23) and men (3.42) (Fig. 1). Men seem to rate working conditions higher than domēna. This difference could indicate that working conditions are perceived differently between the sexes, possibly due to different job demands. Work process, job satisfaction, payment, health, conflict, and digitalization do not show significant differences between the sexes, indicating similar perceptions between women and men (Table I).

TABLE I DIMENSIONS OF THE WORK ENVIRONMENT BY GENDER

	t-test for Equality of Means		
	t	*df*	*Sig. (2-tailed)*
Work process	-,937	113	,351
Work conditions	-2,203	113	,030
Job satisfaction	-1,507	113	,135
Salary	-1,083	113	,281
Health	-,979	113	,330
Conflicts	-1,186	113	,238
Digitalization	-,344	113	,732
Personal life	-2,067	113	,041

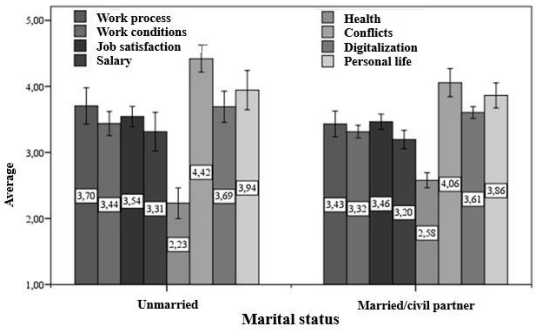


Fig. 2. Dimensions of the work environment by marital status.

Health is the only category where there are statistically significant differences in health perceptions between singles (2.23) and married and being in a civil partnership (2.58) (Fig. 2). Married or in a civil partnership seem to value their health more than singles.

Work process, working conditions, job satisfaction, pay, conflicts, digitalization and personal life - these categories have no significant differences in marital status groups, indicating similar perceptions between singles and married or the one's in a civil partnership (Table II).

TABLE II DIMENSIONS OF THE WORK ENVIRONMENT BY MARITAL STATUS

	t-test for Equality of Means		
	t	*df*	*Sig. (2-tailed)*
Work process	1,415	113	,160
Work conditions	1,232	113	,221
Job satisfaction	,695	113	,488
Salary	,798	113	,427
Health	-2,882	113	,005
Conflicts	1,803	113	,074
Digitalization	,832	113	,407
Personal life	,423	113	,673

Figure 3, reflects how participation in the educational process is an important factor, as there are statistically significant differences in several positions. The first one could be the work process, where the perception of employees who have received education is 3.57, and those who are currently studying is 3.00. Employees with education rate the work process higher than those who are

currently studying. Employees with education probably feel more comfortable with the existing work processes, while those who are currently studying might experience additional challenges in performing work tasks. The second factor could be working conditions, where the perception of employees who have received education is 3.30, and those currently studying 3.62. Employees who are currently studying rate working conditions higher than those who have received education. Employees who are currently studying might feel more satisfied with the working conditions, perhaps they feel support from the employer in the learning process. The third factor could be digitalization, where the perception of employees with education is Mean=3.57, and those currently studying Mean=4.00. Employees who are currently studying rate digitalization higher than those with an education. Employees who are currently are studying are likely to be more updated with the latest technologies and digitalization processes, while those with an education may be less involved. The fourth factor could be personal life, where the perception of employees with an education is 3.96, and those currently studying 3.40. Employees with an education rate personal life higher than those currently studying. Employees with an education may experience a better balance between work and private life, while those currently studying may experience more stress and challenges in trying to balance work and studies.

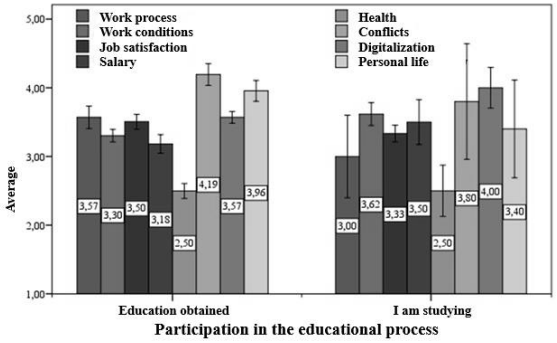


Fig. 3. Dimensions of the work environment by educational process

Job satisfaction, pay, health, and conflict are categories in which there are no significant differences between educational status groups, indicating similar perceptions between employees with completed education and those currently studying (Table III).

TABLE III DIMENSIONS OF THE WORK ENVIRONMENT BY EDUCATIONAL PROCESS

	t-test for Equality of Means		
	t	*df*	*Sig. (2-tailed)*
Work process	2,395	113	,018
Work conditions	-2,548	113	,012
Job satisfaction	1,203	113	,232
Salary	-1,711	113	,090
Health	-,016	113	,987
Conflicts	1,547	113	,125
Digitalization	-3,497	113	,001
Personal life	2,365	113	,020

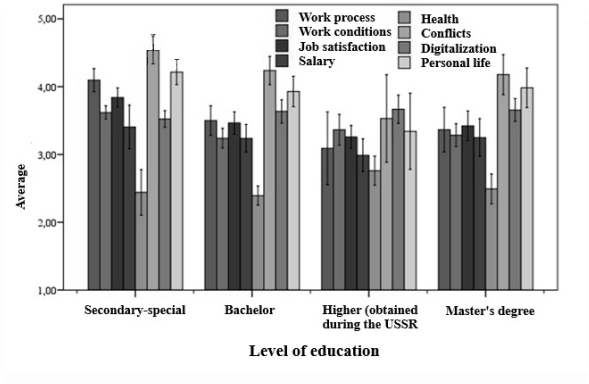


Fig. 4. Dimensions of the work environment by level of education

Education level is an important factor, as it is one of the two questions with the largest number of items where there are statistically significant differences. Work process, working conditions, job satisfaction, conflicts and personal life are categories where there are significant differences between education level groups. The scores of many are lower for employees with higher education, these employees have obtained their education a long time ago, therefore they are also older employees with the most life experience, which could be a factor in different perspectives (Fig. 4).

Remuneration, health and digitalization turned out to be the aspects where there are no significant differences between education levels, indicating similar perceptions among employees with different education levels (Table IV).

TABLE IV DIMENSIONS OF THE WORK ENVIRONMENT BY LEVEL OF EDUCATION

	F	*Sig.*
Work process	5,666	,001
Work conditions	3,736	,013
Job satisfaction	5,506	,001
Salary	1,428	,239
Health	2,210	,091
Conflicts	5,192	,002
Digitalization	,432	,730
Personal life	4,459	,005

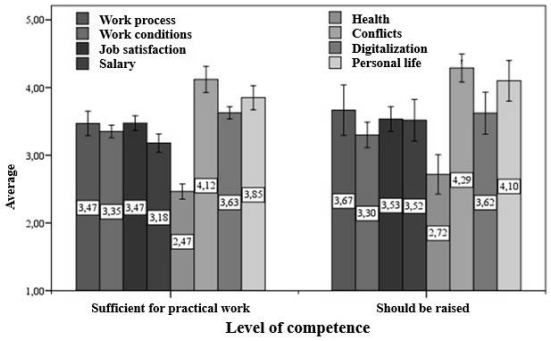


Fig. 5. Dimensions of the work environment taking into account employee's level of competence

There are statistically significant differences in the perception of pay between employees with sufficient competence to perform practical work (3.18) and those needing to increase their competence (3.52) (Fig. 5). Employees with sufficient competence rate their pay lower than those who need to increase their competence. This difference could indicate that employees with a higher level of competence feel less satisfied with their payment, probably because they believe that their skills and abilities should correspond to higher pay.

Work process, working conditions, job satisfaction, health, conflicts, digitalization and personal life - there are no significant differences between the competence level groups in these categories, indicating similar perceptions between employees with sufficient competence and those who need to increase their competence (Table V).

TABLE V DIMENSIONS OF THE WORK ENVIRONMENT BY LEVEL OF COMPETENCE

	t-test for Equality of Means		
	t	*df*	*Sig. (2-tailed)*
Work process	-,808	113	,421
Work conditions	,402	113	,688
Job satisfaction	-,406	113	,685
Salary	-1,818	113	,047
Health	-1,616	113	,109
Conflicts	-,658	113	,512
Digitalization	,034	113	,973
Personal life	-1,045	113	,298

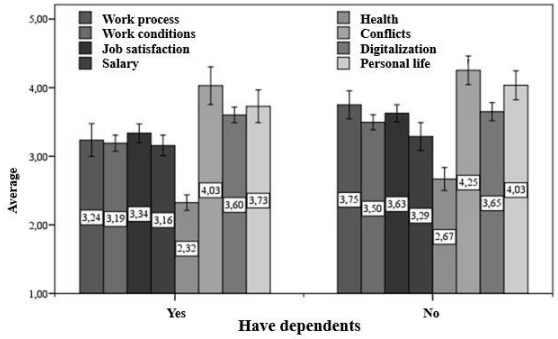


Fig. 6. Dimensions of the work environment for respondents having dependents in the family

The third factor with the largest number of statistically significant differences. In categories where employees have dependent family members on their earnings, ratings are lower compared to those who are single. The t-test results confirm that these differences are statistically significant (Table 6).

The work process is rated significantly higher for employees without dependents (3.75) compared to those with the family members whom they support (3.24). The statistical significance of this difference indicates that additional responsibilities may negatively affect concentration on work. The perception of working conditions is also higher for employees without dependents (3.50) compared to those who undertake responsibility for other family members (3.19). The t-test demonstrate that these differences are statistically significant. This could be due to the possibility for employees without dependents to focus more on improving and adapting the work environment. Job satisfaction also differs statistically significantly. Employees without dependents (3.63) rate their job satisfaction higher than those with dependents (3.34). These differences could be related to less external pressure and responsibilities, which allows them to focus more on work and enjoy its benefits (Fig. 6).

Significant differences are also observed in health perceptions. Employees without dependents (2.67) rate their health status higher than those with dependents (2.32). This could indicate that employees with dependents experience more stress and difficulties that affect their health (Fig. 6)

The perception of personal life between employees with dependents and those without dependents is not statistically significantly different, as the Sig. (2-tailed) value is 0.050, which is right at the accepted limit (0.05). Although the difference between the mean ratings of the two groups (3.73 vs. 4.03) is noticeable (Fig. 6), the t-test indicates that it is not strong enough to be considered significant with high confidence. This result suggests that work-life balance is similar for both groups and although employees without dependents may feel less stressed, this difference is not significant enough to be interpreted as a general trend (Table VI).

TABLE VI DIMENSIONS OF THE WORK ENVIRONMENT BASED ON HAVING DEPENDENTS

	t-test for Equality of Means		
	t	*df*	*Sig. (2-tailed)*
Work process	-3,266	113	,001
Work conditions	-3,812	113	,000
Job satisfaction	-3,126	113	,002
Salary	-1,039	113	,301
Health	-3,400	113	,001
Conflicts	-1,302	113	,196
Digitalization	-,541	113	,590
Personal life	-1,923	113	,050

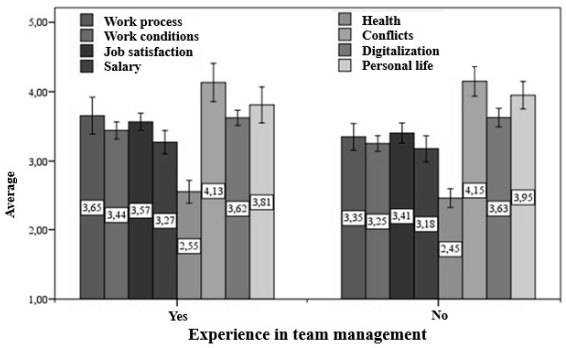


Fig. 7. Dimensions of the work environment by experience in team management

Working conditions is the only category where there are statistically significant differences between employees with experience in team management (3.44) and those without such experience (3.25). Employees with management experience rate working conditions higher (Fig. 7).

Employees with management experience probably feel more satisfied with working conditions because they are more likely to be able to adapt the environment to their needs. Work process, job satisfaction, pay, health, conflict, digitalization, and personal life are categories where there are no significant differences between the management experience groups, indicating similar perceptions between employees with experience in team management and those without such experience (Table VII).

TABLE VII DIMENSIONS OF THE WORK ENVIRONMENT BY EXPERIENCE IN TEAM MANAGEMENT

	t-test for Equality of Means		
	t	***df***	***Sig. (2-tailed)***
Work process	1,880	113	,063
Work conditions	2,258	113	,026
Job satisfaction	1,684	113	,095
Salary	,740	113	,461
Health	,863	113	,390
Conflicts	-,096	113	,924
Digitalization	-,041	113	,968
Personal life	-,872	113	,385

IV. CONCLUSIONS

The conducted research confirms that change management significantly affects the perception of the work environment among senior customs supervisors working at Latgale customs checkpoints. The results showed that socio-demographic factors, such as education level, gender, marital status, the presence of dependents, and experience in managing teams, play a substantial role in shaping employees' views on working conditions, job satisfaction, and overall workplace well-being.

Supervisors with higher education levels demonstrated a more critical attitude towards organizational support and development opportunities. Differences based on gender highlighted varied perceptions of advice, guidance, and work processes, while employees with family responsibilities and team management experience assessed stress levels and career growth differently. These findings emphasize the necessity to consider employees' socio-demographic characteristics systematically when planning and implementing changes in the Customs Board.

The study shows that a uniform approach to personnel management does not fully meet the needs of diverse employee groups. Tailoring management strategies to different employee profiles can improve staff satisfaction, strengthen workplace resilience, and support sustainable change processes in the Customs Board.

Based on the research results, the following recommendations are proposed to improve the work environment and support the personnel management strategy:

Develop flexible workplace policies that consider family responsibilities and promote a healthy work-life balance.

Create targeted training and professional development programs adapted to different educational backgrounds and career stages.

Implement gender-sensitive measures to ensure fairness and equal opportunities in the work environment.

Foster transparency and increase employee participation in decision-making processes to enhance trust and commitment.

Strengthen support programs for employees in managerial positions to reduce work-related stress and improve leadership skills.

The implementation of these recommendations will contribute to improving the efficiency, motivation, and professional well-being of employees, supporting the overall modernization efforts of the Customs Board.

REFERENCES

[1] J. P. Kotter, Leading Change. Boston, MA: Harvard Business School Press, 1996.

[2] S. Fernandez and H. G. Rainey, "Managing successful organizational change in the public sector," Public Administration Review, vol. 66, no. 2, pp. 168–176, 2006. https://doi.org/10.1111/j.1540-6210.2006.00570.x

[3] B. Burnes, *Managing Change*: A Strategic Approach to Organisational Dynamics, 4th ed. Essex, UK: Pearson Education, 2004.

[4] T. G. Cummings and C. G. Worley, Organization Development and Change, 10th ed. Boston, MA: Cengage Learning, 2014.

[5] A. A. Armenakis and S. G. Harris, "Reflections: Our journey in organizational change research and practice," Journal of Change Management, vol. 9, no. 2, pp. 127–142, 2009. https://doi.org/10.1080/14697010902879079

[6] W. Bridges, *Managing Transitions:* Making the Most of Change, 3rd ed. Philadelphia, PA: Da Capo Press, 2009.

[7] K. Lewin, "Frontiers in group dynamics," *Human Relations*, vol. 1, no. 1, pp. 5–41, 1947. https://doi.org/10.1177/001872674700100103

[8] J. Hayes, The Theory and Practice of Change Management, 3rd ed. Basingstoke, UK: Palgrave Macmillan, 2010.

[9] European Commission, Quality of Public Administration: A Toolbox for Practitioners. Luxembourg: Publications Office of the European Union, 2017. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/1e68deed-1c20-11e7-aeb3-01aa75ed71a1[Accessed: Feb. 12, 2025].

[10] A. Hughes, Managing Change in the Public Sector. London: Routledge, 2018.

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 271-276

Speed Tests and Control Exercises in Sports Practice

Sandra Škutāne
Department of Track and Field Athletics and Swimming
Riga Stradins University Latvian Academy of Sport Education
Riga, Latvia
sandra.skutane@rsu.lv

Krišjānis Kuplis
Department of Track and Field Athletics and Swimming
Riga Stradins University, Latvian Academy of Sport Education
Riga, Latvia
krisjanis.kuplis@rsu.lv

Ilze Avotiņa
Department of Track and Field Athletics and Swimming
Riga Stradins University, Latvian Academy of Sport Education
Riga, Latvia
ilze.avotina@rsu.lv

***Abstract* – The theory of testing human physical fitness is one of the most fully developed in the field of sports theory. Of particular importance for the use of test results is the development of various standards. Standards are developed for a certain group of athletes and are valid only for it [1]. The most popular test or control exercise is the 30m run from the high start, a total of four speed ability assessment tests are offered – a 20m run from a high start, a 30m run from a high start, a 60m run from a high start and a 100m run from a high start. Not all sports mention normative results for women and men. Standards in professionally oriented sports, such as boxing, judo, football, hockey, karate, rugby and Nordic combined, are for men only. Such sports as boxing, judo and karate have the same control standards. In turn, in athletics, they are divided according to disciplines. The difference in results during testing is 0.5 seconds, as different systems for recording results are used – with a handheld stopwatch and an electronic result-recording machine. The highest requirements for High Performance Sport groups in the 20m race are set for men in gymnastics – 3.0seconds, and for women in weightlifting – 3.2seconds. The average score in sports where the speed test for the High-Performance Sport group is a 20-meter run from the spot is 3.5±0.19seconds for men and 3.6±0.19seconds for women.**

Coaches of sports schools choose to fix the results with a hand stopwatch. Aim of the study: Evaluation of speed tests and control exercises in sports practice in Latvia.

Keywords – control exercises in sport practice, High-Performance Sport groups (HPS), speed tests.

I. Introduction

The theory of testing human physical fitness is one of the most thoroughly developed areas in sports theory. The development of various standards (norms) is of particular importance for utilizing testing results. Standards are developed for a specific group of athletes and are only applicable to that group [1].

Through testing, it is possible to determine absolute and relative indicators of physical attributes. Absolute indicators characterize the level of development of physical qualities; in this study, we focus on the development level of speed among the High-Performance Sport (HPS) groups.

The Ministry of Education and Science of Latvia (MoES) oversees 36 professional sports disciplines. In 26 of these sports, athletes must perform one of the speed tests: a 20m sprint from a standing start, a 30m sprint from a standing start, a 60m sprint from a standing start, and a 100m sprint from a standing start.

The evaluation of results from control exercises must be conducted annually, and, at least once every 10 years, these results should be reviewed in accordance with the current situation in athlete development.

In the 2020/2021 year, the MES published informative materials for Latvian professional sports education institutions, which are also relevant today for the assessment of control exercise performance Control Standards for Groups of Professional Sports Education Institutions in the Context of the COVID-19 Pandemic [2]. In sports practice, various terms are used that reflect virtually the same concept—control exercises, control tests. In this study, we will use the term control exercises and results instead of the word norms.

II. Materials and Methods

Methods: Analysis of literature sources and scientific studies. Measuring experiment. Mathematical statistical analysis.

Speed in sports training is a person's ability to perform an action in minimal time. Three fundamental forms of speed are distinguished: movement reaction speed, speed

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8478
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

of individual movements, and frequency of movements [3], [4], [5], [6]. These forms of speed are relatively independent of each other. The transfer of speed from one manifestation type to another does not occur [5].

From a biological perspective, the possible movement speed depends on the amount of ATP in the muscles, the rate at which it is broken down under the influence of nerve impulses, and the rate of ATP resynthesis [7]. As emphasized by I. Liepiņš and I. Ķīsis, rapid actions are primarily energetically supported by anaerobic mechanisms, with more than 90% in sprinting [3], [5]. Very fast movements are the result of complex central nervous system activity. The maximum movement frequency primarily depends on the functional state of the nervous system and individual characteristics [8]. I. Pontaga notes that movement frequency is somewhat related to the speed of individual movements because, to ensure a high step frequency, both the agonist and antagonist muscles must contract rapidly in alternation [8], [6]. The method for training movement speed is to perform movements/actions as quickly as possible, using the correct movement technique according to the sport [9]. Speed is determined by movement frequency and the distance covered in a single movement. Maximum speed can be achieved by: 1) choosing optimal relationships between these components mentioned above; 2) specifically increasing one or the other. For example, in running, maintaining a maximum step rate requires increasing the step length; if successful, the running speed increases. Additionally, a runner can achieve an increase in speed by increasing the tempo without reducing the step length [6]. A. Konrads states that in each sport, a person's speed abilities manifest differently. To assess them, specific control exercises unique to each sport must be performed. This is a complex task. In practice, running, especially sprinting, is primarily used as a means of evaluating speed characteristics [6].

In speed characteristic testing, the main measurement is the time indicating how quickly a runner completes a 20m distance. Knowing the distance and the time taken to cover it allows for the calculation of running speed. This is the absolute speed; to achieve maximum speed over the measurable distance, a run-up of at least 20-30 meters is necessary [6].

In sports practice, acceleration is also tested, or the athlete's ability to reach a higher running speed from a standstill as quickly as possible. The greater the acceleration, the better the result [6].

I.Kīsis emphasizes that, based on speed requirements, all sports can be divided into the following categories:

- Sports (sprint distances) that require the maximum development level of all forms of speed in standard situations.
- Sports (team sports) that require the maximum development level of all forms of speed in varied situations.
- Sports (weightlifting, gymnastics) that require a maximum, or near maximum, development level of specific forms under significant external load or complex coordination conditions.
- Sports (skiing, marathon) where the potential for speed expression is heavily limited by endurance [3].

When evaluating any physical qualities, various control exercises can be applied. In sports, the effectiveness of the training process is determined by the use of complex control means and methods as management tools, which ensure feedback between the coach and the athlete [10]. Control exercises should be performed at least twice during the season (at the beginning and end) and twice during training camps [3].

TABLE 1 PHYSICAL FITNESS ASSESSMENT SCALES FOR 18-YEAR-OLD BOYS [4]

Indicators and units	Low level	Medium low level	Medium level	Above med. level	High level
Scores	1	2	3	4	5
Jump (cm)	< 217	218-230	321-241	242-254	> 255
Hanging with bent arms (s)	<2 5.1	25.2-36	36.1-47.1	47.2-58.0	> 58.1
Run 10x5m (s)	> 20. 2	20.1-19.3	19.2-18.2	18.1-17.5	< 17.4
Seat and reach (cm)	< 19	20-23	24-30	31-34	> 35
Hitting the board (s)	> 12. 1	12.0-11.2	11.1-10.5	10.4-9.6	< 9.5
Sit-ups (count 30s)	< 25	26-27	28-29	31-32	> 33
30m run (s)	4.4	4.3	4.2	4.1	4.0
60m run (s)	8.6	8.5-8.3	8.2-8.1	8.0	7.9
300m run (min)	0:5 0	0:49-0:47	0:46-0:45	0:44-0:43	0:42
3000m run (min)	12: 09	12:08-11:58	11:57-11:47	11:46-11:36	11:3 5
Bending and straightening the arms (count)	23	24-25	26-28	29-30	31
Hurdles (s)	16. 9	16.8-16.5	16.4-16.3	16.2-16.0	15.9

Conditions for performing control exercises:

- Exercises should be performed in sports clothing and footwear;
- Exercises must be carried out in a strictly defined order as outlined in the physical fitness assessment, with rest periods between different tests performances;
- Before executing the exercise, athletes should be informed about the conditions of execution to reduce the impact of emotional factors on test results, allowing one attempt to familiarize themselves with the execution and ensure that the rules are understood (except for middle and long-distance tests);

- Exercises should be conducted in a competitive format, requiring precise and rapid execution [3].

Control Exercises "30m Sprint and 60m Sprint" – for determining running speed. A stopwatch is required for conducting the tests. Preparation for executing the test: athletes stand behind the line, placing one foot directly on the line (starting from the blocks). After the signal, they sprint as fast as possible to the finish line, which is located 30m or 60m away, and cross it. The stopwatch is stopped when the athlete crosses the finish line. The control exercises are performed simultaneously by two athletes. Results – sprint times in tenths of a second – are recorded on a results sheet. Each control exercise is conducted twice, and the best result is considered (Ķīsis, 2015). The same method for determining running speed is used for the 20m and 100m sprints. Nowadays, the recording of control exercise results is done using electronic timing devices, rather than hand-held stopwatches, although using a hand-held stopwatch is not prohibited. The use of smartphones for recording results is not allowed.

I. Ķīsis (2015) offers results that should be presented for 18-year-old boys (see Table 1). The results have 5 levels, which are informative for students to assess their level of preparedness. No equivalent results table is provided for girls.

A. Rudzītis and V. Lāriņš note that scientists from various countries have accumulated a considerable amount of information indicating that results applicable, for example, to adolescents and young adults in the northern European countries cannot be used in southern European countries or on the African continent [1]. The results are characterized by their representativeness, which means that it is still possible to develop results that can be applied to athletes from different geographical regions. Another aspect that interests researchers is the relevance of the results (norms, standards). In practice, it is accepted to review the results no less frequently than once every 10 years. This allows scientists to assess the trends in athlete development.

In 2008, A.Rudzītis et al. stated that in Latvia, no scientifically based norms had been developed in the last 10 years to evaluate the physical fitness of young athletes [1]. In the 2020/2021 academic year, the Ministry of Education and Science prepared and sent sports schools an informational material titled Control Standards for Groups of Professional Sports Education Institutions in the Context of the COVID-19 Pandemic [2].

TABLE 2 30M RUN RESULTS FOR 16 – TO 19-YEAR-OLDS (DAVIS, 2000) [11]

Gender	High level (s)	Above average level (s)	Average level (s)	Below average level (s)	Low level (s)
Male	< 4	4.0 – 4.2	4.3 – 4.4	4.5 – 4.6	> 4,6
Female	< 4,5	4.5 – 4.6	4.7 – 4.8	4.9 – 5.0	> 5.0

B. Davis (2000) published results from his country for young people aged 16 to 19 years (see Table 2)[11].

Comparing the assessment of the 30m sprint results presented by I. Ķīsis (2015) and the results obtained during the 30m sprint by B. Davis (2000), we see that the results are very similar. A High-Performance level in both cases is 4.0 seconds; although the tests are different, the athlete can achieve a higher result during the sprint.

Based on the obtained results, it is possible to:

- compare the preparedness of individual students as well as groups of athletes;
- organize the selection for training groups;
- implement objective pedagogical control of the training process's effectiveness;
- assess the appropriateness of training means, methods, and forms of organization;
- justify physical fitness standards [1].

With the help of control exercises, it is possible to determine absolute and relative indicators of physical attributes. Absolute indicators characterize the level of development of physical attributes, specifically the level of speed development in HP groups in this study.

Ethics. Before commencing the theoretical study, an opinion was received from the Ethics Committee of Riga Stradins University, No 2-PĒK-4/293/2025, stating that the research would be conducted in accordance with the regulations concerning the adherence to ethical norms in scientific research. The theoretical study took place from January 6, 2025, to January 31, 2025.

Theoretical analyses were conducted on control exercises for determining running speed among students in Professional Orientation Sports Schools' HPS groups. The control exercises can help ascertain absolute and relative indicators of performance. Absolute indicators characterize the level of development of physical qualities; in this study, the focus was on the level of speed development among the HPS groups across four speed tests or control exercises. Running speed is considered an absolute or evident indicator [1]. These are simple control exercises according to the classification of control exercises; these exercises involve a single movement task – to cover a specified distance as quickly as possible.

In sports performance measurements, the limits of test results are considered the standard, which allows athletes to be categorized into specific qualification groups or levels of preparedness (Rudzītis et al., 2008).

The basis of the study was provided by the Cabinet of Ministers Regulation No. 508, "Procedure for State Funding of Professional Orientation Sports Education Institutions," Appendix 1 – Requirements for Effectiveness Criteria [12].

The obtained data were processed using simple statistical methods, calculating the mean and standard deviation. The results were compared and analysed against the data mentioned in the literature.

III. Results and Discussion

Out of 36 sports, athletes in the HPS group must perform speed tests in 26 sports: a 20m sprint from a standing start, a 30m sprint from a standing start, a 60m sprint, and a 100m sprint from a standing start [2].

The 20m sprint from a standing start is included as a control exercise in the following sports in specialized sports schools: basketball, BMX, cycling, artistic gymnastics, and weightlifting. In these sports, there is a specific running action that authors mention in studies or articles, and, accordingly, the sports schools have chosen the corresponding exercise [2].

The 30m sprint from a standing start is included as a control exercise in the following sports in specialized sports schools: badminton, biathlon, boxing, cross-country skiing, judo, football, table tennis, handball, hockey, karate, fencing, rugby, tennis, volleyball, and Nordic combined [2].

The 60m sprint from a standing start is included as a control exercise in the following sports in specialized sports schools: boxing, figure skating, judo, karate, rugby, and athletics [2].

The 100m sprint from a standing start is included as a control exercise in the following sports in specialized sports schools: sailing, judo, karate, modern pentathlon, orienteering, and short track [2].

From the above, it can be seen that the most popular control exercise is the 30m sprint from a standing start. Not all sports mention performance results for women and men. Results in specialized sports such as boxing, judo, football, hockey, karate, rugby, and Nordic combined are only available for men.

In the 30m sprint from a standing start, the highest results for HPS groups are noted in Nordic combined and rugby for men – 4.0 seconds (see Fig.1).

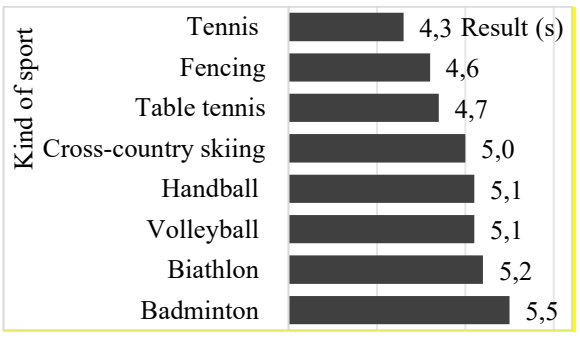


Fig. 1. Results in the women's 30m run.

For women, the fastest result in the 30m sprint is recorded in table tennis – 4.3 seconds (see Fig.2). The average result for men in the 30m sprint is 4.8 ±0.19 seconds and for women, it is 5.1 ±0.33 seconds.

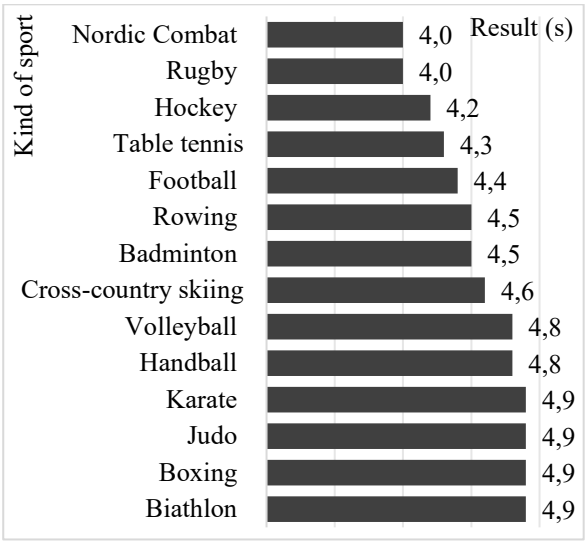


Fig. 2. Results in the men's 30m run.

The best results in the 60-meter sprint for both men and women should be presented by track and field athletes – sprinters and jumpers. 7.7 seconds for men and 8.7 seconds for women. The average result in the 60-meter sprint is 8.6 ± 0.5 seconds for men and 9.0 ± 0.21 seconds for women (see Fig. 3 and Fig. 4).

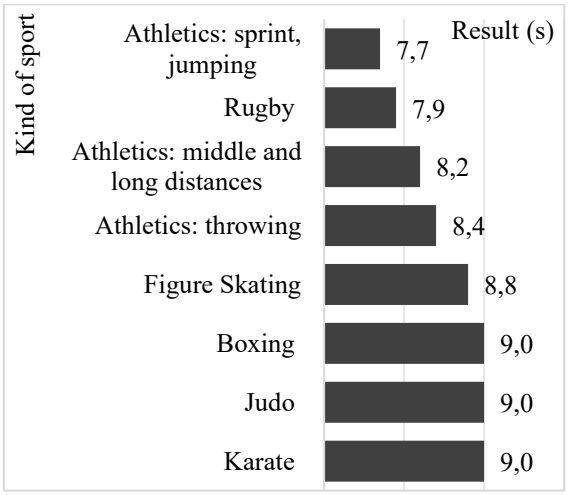


Fig. 3. Results in men's 60m run.

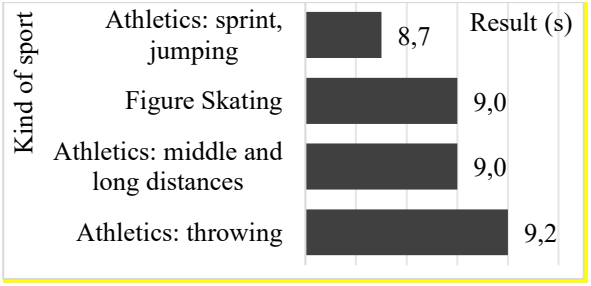


Fig. 4 Results in the women's 60m run.

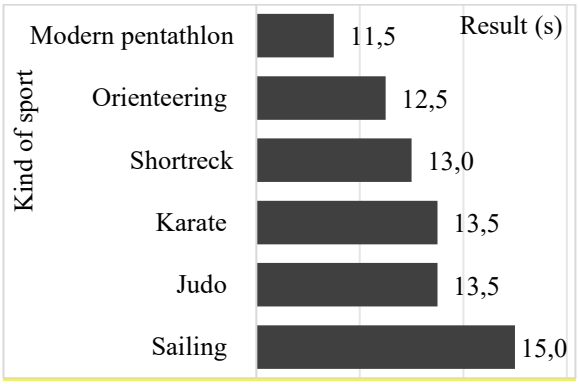


Fig. 5. Results in men's 100m run.

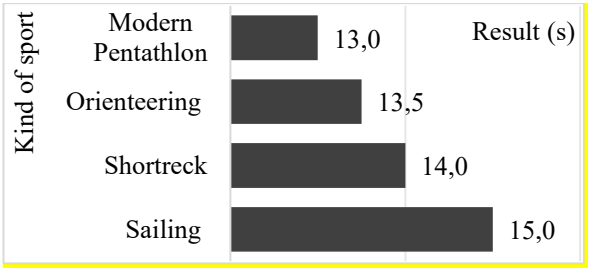


Fig. 6. Results in women's 100m run.

In the 100-meter sprint, the average result for men is 13.3±1.25 seconds and for women it is 14.0±1.0 seconds. The fastest times in the 100 meters for both men and women should be shown in modern pentathlon – 11.5 and 13.0 seconds, respectively (see Fig. 5 and Fig. 6).

The highest standards for HPS groups in the 20m sprint for men are set at 3.0 seconds in gymnastics (see Fig. 7), while for women in weightlifting, it is 3.2 seconds (see Fig. 8). The average result in sports where the speed test for the HPS group is a 20-meter sprint from a standing start is 3.5 ±0.19 seconds for men and 3.6 ±0.19 seconds for women.

In summary, as previously described, we can observe that sports federations choose the 30m sprint as a control exercise—14 sports for men and 8 sports for women (see Table 3). The numerical values of other speed control exercises can be seen in the same table.

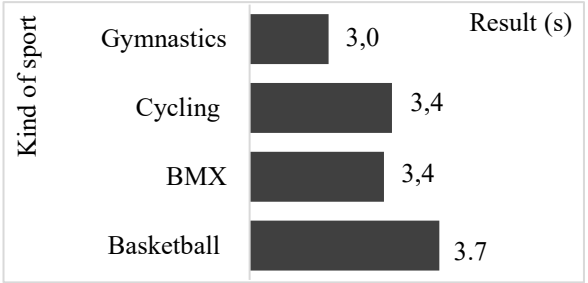


Fig. 7. Results in men's 20m run.

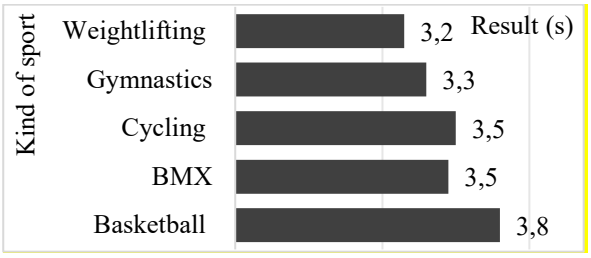


Fig. 8. Results in the women's 20m run.

Analysing the differences in the results of the indicated control exercises in different sports, it should be concluded that they are significant. It can also be concluded that in most sports there are minimal requirements for achieving high-quality results in speed control exercises. Such differences are explained by the fact that the results of the control exercises to be achieved are determined by the federations of each sport at their own discretion, based on different principles. The control exercises offered by sports federations shall be performed at least once a year and approved by the Ministry of Education and Science, and they shall be considered as corresponding to the specifics of the sport, as well as shall be executed by students of the High-Performance Sport group.

IV. Conclusions

Analysing the differences in the results of the specified control exercises across various sports, it can be concluded that these differences are significant. It can also be inferred that in most sports, the requirements for achieving high-quality results in control exercises are minimal. Such differences can be explained by the fact that the target results for control exercises are determined by the federation of each sport at their discretion, based on different principles. The control exercises proposed by the sports federations must be performed at least once a year and are approved by the Ministry of Education and Science; they are considered appropriate to the specifics of the sport and are executable by the trainees of the High-Performance Sport group.

There is no specific measuring instrument for recording results. This can be done with a handheld stopwatch or by using specialized timing electronic devices. It should also be noted that there is no standardized terminology for the representation of control exercises and results in literature data.

A debatable question is whether the running speed control exercises are suitable for all sports in which they are used. In the HPS groups of sports schools, the greatest emphasis in physical preparation is placed on special fitness, and the correlation between fast running and competition results is minimal in most sports. For the youngest groups of trainees, the results of short distance running and their dynamics are significantly more important. Of course, there are sports (athletics, football,

rugby) where movement speed is very important for achieving high performance in competitions.

REFERENCES

[1] A. Rudzītis un V. Lāriņš, "Basketbolistu fiziskās sagatavotības kontrole un rezultāti", Bērnu un pusaudžu trenera rokasgrāmata, Rīga: LTTC, 2008, 124-137 lpp.

[2] Profesionālās ievirzes sporta izglītības iestāžu grupu kontrolnormatīvi COVID – 19 pandēmijas apstākļos (2020), Informatīvais materiāls Latvijas profesionālās ievirzes sporta izglītības iestādēm 2020/2021 m.g.,

[3] I. Ķīsis, Sporta teorija 2. daļa, Rīga: LSPA, 2002, 24-25 lpp.

[4] I. Ķīsis, "Fiziskās sagatavotības noteikšana un novērtēšana" Vispusīgās fiziskās sagatavotības trenera rokasgrāmata*,* Rīga: SIA DUE, 2015, 28-30, 33, 41 lpp.

[5] I. Liepiņš, Ātrums un tā attīstīšana, *Sports un treniņš*, Rīga: autora izdevums, 2000, 181.-182. lpp.

[6] A. Konrads, "Ātruma treniņš", Trenera rokasgrāmata, Rīga: LTTC, 2003, 68-69 lpp.

[7] F. Bosch and R. Klomp, Generation of energy. Running. Biomechanics and Exercise Physiology Applied in Practice. Churichill Livingstone, Elsevier, 2007, pp. 83 – 84.

[8] I. Pontaga, Spēka, spēka izturības, ātrspēka un ātruma attīstīšanas fizioloģiskais pamatojums*. 1.daļa,* Rīga LSPA, 2023, 56-58 lpp.

[9] C. Boreham, The Physiology of Sprit and Power Training. Chapter 6 in: *The Physiology of Training*, Churichill Livingstone, Elsevier, 2006, pp. 117-134.

[10] A. Fernāte, Fiziskā sagatavošana, Sporta treniņu teorijas pamati. 2.daļa*,* Rīga: LSPA, 2002, 15, 73 lpp.

[11] B. Davis, Physical Education and the study of sport. 4th ed. London: Harcourt Publishers, 2000, p. 125.

[12] Ministru kabineta noteikumi Nr. 885, Rīgā 2021. gada 21. decembrī (prot. Nr. 81 79. §) Kārtība, kādā valsts finansē profesionālās ievirzes sporta izglītības programmas, pieejams: www.likumi.lv Kārtība, kādā valsts finansē profesionālās ievirzes sporta izglītības programmas [Skatīts: 2025.gada 13.janvarī].

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 277-284

Integration Processes in the Military Education System

Milko Stefanov
Rakovski National Defense College
Sofia, Bulgaria
m.j.stefanov@rndc.bg

Daniel Berchev
Research and Innovation Institute
Vasil Levski National Military University
Veliko Tarnovo, Bulgaria
dberchev@nvu.bg

***Abstract* — This article explores the integration processes within military education systems, emphasizing their critical role in modernizing curricula and addressing the dynamic needs of national and international security. The aim is to analyze integration models and strategies that combine civilian and military education, theoretical and practical training, and traditional and innovative teaching methodologies. Using a systematic and comparative approach, the study evaluates global practices and specific examples from Bulgaria and NATO member states to identify effective integration strategies.**

The research highlights the importance of fostering synergy between diverse educational components to enhance the preparation of military personnel for evolving defense challenges. Integration models, such as dual and modular training and institutional cooperation, are analyzed for their potential to combine military and civilian expertise. The integration of theoretical knowledge with practical training, including the use of simulations, field exercises, and joint international training, is shown to be critical for developing problem-solving skills and operational readiness. Furthermore, balancing traditional and innovative teaching methods is identified as a means to foster critical thinking and adaptability in learners.

The study concludes that integration is a strategic imperative for modern military education. Key recommendations include strengthening collaboration between military academies and civilian institutions, continuously updating curricula to reflect technological advancements, increasing opportunities for practical training, promoting flexible learning models, and investing in resources such as equipment, facilities, and teacher development. These measures are essential for preparing military professionals to meet the complexities of contemporary defense and security environments effectively.

Keywords* — *civilian-military cooperation, integration processes, military education system, theoretical and practical training.

I. Introduction

Integration in military education is a topic of growing importance in contemporary educational systems worldwide. Integration is defined as a dynamic process of uniting different elements into a cohesive whole, aimed at achieving synergy and unlocking new opportunities. Within military education, this process is strategic, driven by the need to modernize curricula, promote interdisciplinary knowledge, and balance theoretical and practical training to meet the demands of the rapidly changing defense and security environment.

Using a comparative analysis of global practices and specific examples from Bulgaria and NATO member states, the article aims to analyze contemporary integration models in the military education system and to propose strategies for their optimization. Using a systematic approach, the study evaluates the integration of civilian and military education, theoretical and practical training, and traditional and innovative teaching methodologies.

Examining integration from multiple dimensions, the authors argue in the article that integration in military education is not simply an organizational or pedagogical necessity, but a strategic imperative. By promoting interconnectedness between disciplines, institutions, and methodologies, military education can better prepare individuals in the armed forces for complex, multidisciplinary challenges in the context of national and international security.

II. Materials and Methods

A comparative analysis of different models of military education systems, including those in Bulgaria and NATO countries, was used to identify common trends, differences and best practices in integration processes.

A systematic analysis was applied to establish the interaction between the different components and how

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8466
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

integration can improve the effectiveness of the military education system as a whole.

An analysis of documents, such as higher education development strategies, laws and regulations, was carried out to establish the goals, policies and mechanisms for integration in military education.

An analysis of existing practices of different models of integration that are applied in practice, such as dual training, modular training and cooperation between institutions, was carried out. This approach allows illustrating the different ways in which integration is implemented in military education.

III. Results and Discussion

1. Fundamentals of integration processes

1.1. The concept of "integration" in the context of education

Integration in the broad sense of the word is a process of uniting disparate parts into a common, unified and whole, and contributes to increasing efficiency and productivity [1, p. 112]. Furthermore, integration is a process that is characterized by multi-facetedness and multi-layeredness. It is not simply the collection of parts, but their fusion into a single whole, in which differences are overcome or become complementary elements, through interaction and interdependence. The purpose of integrating the elements of the system is to create a synergistic effect that leads to the creation of new properties and capabilities that are not inherent in the individual parts. This is achieved by creating stronger connections between people, organizations, and systems. On the other hand, by combining different elements, integration can lead to the emergence of new ideas and opportunities. In this way, applied in many fields, from science and technology to the humanities, it becomes the driving force of development and progress. This gives us reason to claim that integration is a universal process that is relevant to all aspects of our lives. In support of this statement, we can point out that we are talking about integration in the social, economic, cultural, and technological spheres.

But when we consider the issue of integration in the field of education, the goal is to achieve new knowledge by combining knowledge from different fields. This is a complex process that goes beyond the simple collection of different elements.

Depending on what elements are combined and in what way, there are different types of integration in education. Andreev, M. considers three main types: vertical, horizontal and functional integration [2, p. 386].

According to the author, vertical integration in education refers to connecting different levels of education in a way that ensures a smooth transition and better absorption of knowledge. The advantages are better understanding of the processes, deeper knowledge and motivation to upgrade them. Vertical integration in education is an important tool for creating a connected and effective education system.

Horizontal integration in education is the linking of different academic disciplines or areas of knowledge within the same educational level. The aim is to create more comprehensive and meaningful educational products for learners by showing how different subjects are related to each other and how they can be applied in real life.

Functional integration in education is the linking of different aspects of the learning process. It is a tool for creating dynamic and effective learning that allows learners to see how the knowledge they acquire is useful in real life and to develop skills that they will need in the future. This can involve integrating different subjects, teaching methods, technologies, or even different educational institutions.

The analysis shows that, in addition to everything said so far, integration in education is a strategic approach aimed at creating an educational environment that is diverse, effective and responsive to the needs of the education system. Through it, not only knowledge and skills are developed, but also key competencies such as critical thinking, creativity, collaboration and communication.

For example, the "Strategy for the Development of Higher Education in the Republic of Bulgaria for the Period 2021-2030" [3] sets out activities and measures to achieve the goals, which cover a wide range of aspects, ranging from the modernization of curricula and programs, through improving the quality of teaching and research, to internationalization and strengthening the connection between education, science and business. The main directions are the development of competencies, digitalization, interdisciplinarity and practical orientation of training. In addition, the aim is to increase the mobility of students and teachers, attract foreign students and integrate into international educational and scientific networks. The strategy also envisages closer cooperation between universities, business and the state in the fields of education, research and innovation.

Development strategies in the military education system are a function of the "Strategy for the Development of Higher Education in the Republic of Bulgaria". For example, the main characteristics of the educational process at the Vasil Levski National Military University (NMU "Vasil Levski"), specified in the "Strategy of the Vasil Levski National Military University 2030" [4], show that the emphasis is placed on the evolution of the process, highlighting both the permanent elements and the changes determined by the historical and social contexts.

The Military University has always been focused on training qualified officers, taking into account national priorities and the traditions of the army. The duration of training and the structure of the academic year have varied over the years, but there has always been a striving for a balance between theoretical and practical training, with one of the distinctive features of military education being the

combination of general education subjects with intensive military training.

The analysis reveals two main approaches to organizing the learning process:

- individual approach – initial general training, followed by specialization. This approach is characteristic of earlier periods, but also manifests itself as a contemporary trend.

- specialization at the beginning of education – narrow specialization from the first year, with the accompanying less flexibility. This approach was dominant during certain periods of the mid-twentieth century.

Today, emerging trends are for greater flexibility in curricula and a striving for a balanced combination of academic knowledge and practical military skills. The strategy relies on the development of leadership qualities, communication skills and emotional intelligence, as well as the integration of digital tools and simulations in the learning process.

The development strategy of the Rakovski National Defence College also relies on integration processes in several aspects in order to meet the high requirements of modern defense and security [5]. First of all, this is the integration of military and civilian education, through the development of joint educational programs, exchange of teachers and joint scientific research. Next is the integration of theoretical training with practice, through closer cooperation with the armed forces, introduction of new technologies, internships and practices. The Rakovski National Defence College envisages in its strategy for the development and updating of curricula and programs in accordance with the requirements of NATO and other international organizations, participation in international projects and cooperation with foreign military academies. Attention has also been paid to the integration of different types of learning, through the development of distance learning and the use of a combination of traditional and innovative teaching methods to meet the different needs of students.

1.2. The systems approach in education

The systems approach is often used to justify integration processes in education. The most operationalized concepts of the systems approach for the needs of education are connection and systematization [2, p. 388].

The systems approach is a way of thinking and analysis that views objects as systems – collections of interconnected elements that interact with each other and with the environment. This approach is widely applied in various fields, including education, and is guided by certain principles.

Berchev, D. and Stefanov, M. provide a broader definition, considering the systems approach in the context of the military education system and doctrinal documents [6].

Within the Armed Forces of the Republic of Bulgaria, the systems approach to training has been defined as a model for managing individual and collective training in order to control the quality of training and the quantity of resources allocated for training and preparation of the headquarters and formations of the Armed Forces. This is an analytical method that determines what training should be carried out with personnel, headquarters and formations to reach certain standards that guarantee the successful execution of tasks in crisis response operations and to ensure national security [7, p. 23].

The analysis of this definition outlines the following aspects. First of all is the formulation of the goal – optimization of the process of training of personnel, headquarters and formations, which guarantees high standards and efficient use of resources. Next is the use of an analytical method to determine the type of training to achieve the specific goals, as well as the scope of application and the benefits of its implementation.

The definition also reflects some of the basic principles of the systems approach – goal-orientedness, complexity, resource optimization and quality control.

The application of the systems approach in education allows the learning process to be considered as a complex system consisting of learners, teachers, learning materials, teaching methods, environment, etc. Analysis of the interrelationships between these elements allows to improve the efficiency of the educational process and achieve better results.

The systems approach is a tool for identifying problems and seeking effective solutions. It can be used to assess the impact of various changes in the system and to develop a more holistic and integrated approach to education.

Berchev and Stefanov substantiate the claim that the systems approach to education is a set of integration processes [6]. They are related concepts, especially in the context of education as a complex system. This allows problems and processes to be viewed as whole systems, rather than as isolated elements. This is essential for integration, as it requires the connection of different components to achieve a common goal. In addition, the systems approach emphasizes the importance of interactions between the different elements of the system. In integration processes, understanding these interactions is key to successfully connecting the different components. Understanding the structure of the system and how the different elements are organized enables us to plan and execute the integration processes. The systems approach takes into account the dynamic nature of systems. Integration processes are also dynamic and require continuous adaptation to changing conditions.

In summary, the systems approach and integration processes are inextricably linked. The systems approach provides the necessary tools to analyze and manage integration processes, while integration, in turn, allows for more efficient and sustainable systems to be created.

2. Analysis of existing integration processes in the military education system

Educational system models represent different ways of structuring and organizing the learning process. Each of them has its own specific characteristics and advantages [8].

Most of the existing examples relate to the school education system, but they nevertheless give us valuable information about trends in education systems.

For example, analysis of the education systems in Shanghai, the Netherlands and Estonia shows different approaches to the organization and delivery of education, with an emphasis on individualization, practical learning and flexibility in student choice. Characteristic of the education systems in other countries such as Finland and Canada is that they emphasize the importance of holistic development, equity in education and adaptability of assessment methodologies, resulting in high levels of education and international success [9, 10].

Existing models of educational systems have not only their advantages, but also suffer from disadvantages. The optimal choice of model depends on the specific educational situation and the goals it sets for itself. In the modern educational environment, there is an increasingly common trend towards combining different models to create more flexible and individualized curricula.

In view of what has been said so far, the choice of an appropriate educational model for military training is a complex issue that depends on numerous factors, including the specifics of the military profession, the objectives of the training, as well as the dynamic environment in which the armed forces operate. Traditionally, military education has followed a more linear model. This means that training takes place in a strictly defined sequence of courses (curriculum disciplines) and topics, starting with basic military disciplines and progressing to more specialized knowledge and skills. This model provides a solid foundation of military knowledge and skills, but may not be flexible enough to respond to the rapidly changing military environment. To this end, military education needs flexible and adaptable models that respond to the dynamic environment and prepare military personnel for successful performance of their tasks.

The analysis of the models of military education systems in some of the NATO member countries shows precisely these trends.

The U.S. military education system is characterized by a hierarchical, multi-tiered approach. It is designed to develop military leaders through a structured and progressive continuum of training and education throughout their careers. Education begins with undergraduate training at institutions such as the United States Military Academy at West Point, the Naval Academy, and the Air Force Academy. Mid-career training is provided at the Command and General Staff College (CGSC), and advanced strategic training is provided at the National Defense University (NDU). The emphasis is on developing leadership, technical expertise, and academic rigor, and in the preparation of senior officers, training at higher levels of education, the curriculum focuses on military strategy, operations, and politics. Field training is also an integral part of U.S. military education [11, pp. 37-44].

The United Kingdom's military education model integrates civilian education with military officer training. Key institutions include the Royal Military Academy Sandhurst (for the Army), Britannia Royal Naval College (for the Navy) and Royal Air Force College Cranwell (for the Air Force). This system combines academic training with military field training, leadership development, and critical thinking. Officers can earn advanced degrees from accredited universities in relevant civilian fields while in service, encouraging intellectual flexibility and interdisciplinary knowledge.

Germany relies on a dual approach of academic-military education, with officers receiving degrees from the Bundeswehr University in Munich and Hamburg. These universities operate as civilian academic institutions but meet military needs. This system is characterized by an emphasis on technical and engineering education, encouraging the development of analytical skills, technical proficiency, and operational efficiency. Officers receive civilian-equivalent degrees along with military training [11, pp. 46-47].

The French military education system relies on leading institutions such as the École Spéciale Militaire de Saint-Cyr (for the Army), the École Navale (for the Navy), and the École de l'Air (for the Air Force). Senior officer training includes advanced strategic courses at the École de Guerre (War College). Officers progress through undergraduate, mid-career, and senior officer education. The education system emphasizes a holistic approach, including military training, academic education, and leadership development. In addition, French military education also emphasizes “formation humaine” (human development), focusing on moral education, critical thinking, and leadership [11, pp. 48-52].

However, current trends point to an increasing need to combine different models in order to ensure greater flexibility and efficiency. It is important to note that the choice of an appropriate educational model depends on the specific conditions and goals. This is clearly evident from the examples given of the military education systems of some NATO member states. Here it should be emphasized that they reflect the combination of national military needs and NATO strategic objectives, promoting operational readiness, technical expertise and joint interoperability. Each country adapts its education system to balance domestic military priorities with NATO's multinational operational requirements.

2.1. Integration of civilian and military components in training

Recently, efforts to change the higher education system have definitely intensified [12, p. 86]. The integration of civilian and military components in training is one of the

processes that is actively developing in the Bulgarian military education system. The goal is to create highly qualified specialists capable of responding to contemporary challenges to national security and functioning effectively in multinational environments.

The **Dual training model** is regulated in the Law on Defense and Armed Forces of the Republic of Bulgaria, where in Art. 95, Para. 5 it is stated that "When training in military specialties, military academies and higher military schools also conduct training in a relevant accredited civilian specialty and award the relevant educational and qualification degrees in accredited military and civilian specialties." [13]. In addition, Art. 3, Para. 3 of the Regulation on the State Requirements for Acquiring Higher Education with a Bachelor's Degree in the Professional Field of Military Affairs in the Specialties of the Regulated Profession of Tactical Level Command Officer states that training is provided "in specialties of the professional field of Military Affairs and in specialties of other professional fields, with training being conducted according to unified curricula." [14].

This model is applied in all higher military schools in the Republic of Bulgaria and assumes that students receive both civilian and military education, as well as a diploma for a civilian and military specialty.

Modular training model

This model is common and conceptually resembles the dual education model, but the emphasis is only on a separate part (a subject, a separate semester), not on an entire specialty.

For example, at the NMU "V. Levski", with the adoption of the 2022 curriculum for cadets from the military specialization "Motorized Infantry and Tank Troops"; "Intelligence" and "Military Police", who are also trained in the civilian specialty "National and Regional Security", two common modules are included:

- Common Module – Common Security and Defense Policy (CSDP) – 18 hours of lectures, 18 hours of exercises (total 36 hours) – studied during the winter semester of the 4th year;

- Common Module – Troop Leading Procedures – 21 hours of lectures, 9 hours of exercises (Total 30 hours) – studied during the winter semester of the 5th year.

These two modules are also studied in some of the universities that are partners of the NMU "V. Levski" under the Erasmus+ program.

Another example is the creation of the "European Joint Technical Semester for Defence and Security" (EuCTS_DS). This initiative became an Erasmus+ project, implemented in the period 01.12.2020 – 30.11.2022. The project involves the Military Technical Academy "Ferdinand I" of Bucharest, Romania; Military University of Technology Warsaw, Poland; Hellenic Air Force Academy, Athens, Greece; Vasil Levski National Military University, Bulgaria – Faculty of Artillery, Air Defense and CSI; French Air Force Academy, Salon de Provence, France. The objectives of the project are the development, testing and design of a new modular curriculum for an international technical semester in defense and security, at bachelor's level, common to the European Union, as well as the development of a network of lecturers with competences in the field of technical defense and security systems.

Last but not least, the example that can be cited is with the curricula of civilian universities that include military modules, such as courses in military history, strategy, logistics or international relations, especially in specialties such as national security, international relations and political science.

Model of cooperation between institutions

This model involves cooperation between civilian universities and military academies through:

1. Joint scientific research – scientists from both sectors collaborate on projects related to national security. An example of this model is the implementation of the National Scientific Program "Security and Defense", in which the Center for National Security and Defense Studies – Bulgarian Academy of Science, University of National and World Economy (UNWE), University of Library Science and Information Technologies (UniBIT), Rakovski National Defence College, Defense Institute "Prof. Tsvetan Lazarov", Academy of the Ministry of Interior, Higher Naval School "N. Y. Vaptsarov", National Military University "Vasil Levski", Higher Air Force School "G. Benkovski", Laboratory Complex at the Science and Technology Park "SOFIA TECH PARK" and other higher schools and scientific organizations participate. The program was created in implementation of the National Strategy for the Development of Scientific Research 2017-2030 (NSDSR) with the aim of increasing the national scientific capacity in the field of security and defense. The consolidated efforts of the aforementioned scientific organizations, higher education institutions and innovative business organizations are aimed at achieving real scientific results, giving the Republic of Bulgaria a competitive advantage in specific segments of security, cybersecurity and defense of the Republic of Bulgaria, the EU and NATO.

2. Exchange of teachers – teachers from civilian universities can teach at military academies and vice versa. This model is mainly implemented through the exchange of teachers under the Erasmus+ program. But in the last 2-3 years, with the introduction of the possibility of creating joint curricula between higher education institutions, collaboration between civilian and military universities has been observed. As an example, we can point to the NMU "B. Levski", which educates students in joint master's programs with Sofia University "St. Kliment Ohridski" and Southwestern University "Neofit Rilski", thus realizing an exchange of teachers and students.

TABLE 1 ADVANTAGES AND DISADVANTAGES OF MODELS OF INTEGRATION OF MILITARY AND CIVILIAN COMPONENTS IN TRAINING

Model	Advantages	Disadvantages
Dual training	- Broader perspective; - Better understanding of complex issues	- Longer training; - Higher demands on learners
Modular training	- Flexibility; - Ability to choose specialization	There may be a lack of integrity in training
Cooperation between institutions	- Synergy between civil and military knowledge; - Research opportunities	Bureaucratic obstacles may arise

Table 1 shows the advantages and disadvantages of models of integration of military and civilian components in training. This process has great potential to improve the quality of education and prepare specialists capable of dealing with complex security problems. The choice of an appropriate model depends on the specific conditions and objectives. It is important to note that successful integration requires cooperation between different institutions, as well as flexibility and adaptability to changing conditions.

2.2. Integration of theoretical and practical training

The integration of theoretical and practical training is a key aspect of modern military education. It aims to create not only theoretically prepared specialists, but also individuals capable of applying their knowledge in real-world conditions.

Several approaches are used in the military education system. In the modular approach, theoretical modules alternate with practical classes, allowing cadets to immediately apply what they have learned. The use of simulators for training in shooting, driving vehicles (tracked and wheeled), making tactical decisions, etc. is increasingly being used. A key aspect of implementing this approach is regular training exercises, where theoretical knowledge is applied in conditions close to combat.

In project-based learning, students work on projects that require a combination of theoretical knowledge and practical skills. Case studies are another aspect of this approach, which involves analyzing real or simulated situations that require decision-making.

In the approach to completing internships and practices in military units, cadets have the opportunity to become familiar with daily work and acquire practical skills.

As a summary, we can point out that the integration of theoretical and practical training can also be realized through:

- **Using simulation centres**. In some higher military schools, such as the NMU "V. Levski", the Higher Naval School "N. Y. Vaptsarov" and the Rakovski National Defence College, simulation centers have been created where students can practice various scenarios. These are of the type of so-called constructive simulation systems, which are distinguished by the fact that when working with them, participants have the opportunity to control software-simulated units by submitting commands from the interface of their workstation, and then observe the results of their decisions on the screen, namely how their virtual subordinates act with virtual equipment, vehicles and weapons to perform the assigned tasks. In the armed forces of NATO member states, one of the widely used software applications for constructive simulation at the tactical level is JCATS (Joint Conflict and Tactical Simulation), and at the operational and strategic level – JTLS (Joint Theater Level Simulation) [15, pp. 321-322].

- **Conducting exercises at training ranges.** This is related to the Experiential Learning Model (ELM), which is a form of learning based on the principle of acquiring knowledge through experience. As individuals in the armed forces of any country face physical and mental challenges, experiential learning promotes better understanding and extraction of knowledge from experience. ELM can be applied to military training in a four-step cycle described by David Kolb: 1. Concrete Experience; 2. Reflective Observation; 3. Abstract Conceptualism; 4. Active Experimentation. Overall, this cycle embodies a learning process that gives knowledge from experience and turns into useful information [16]. This is fully responsible for the training of the cadets from the NMU "V. Levski", who are scheduled to regularly participate in exercises at training ranges, where they apply the acquired knowledge and improve their practical skills.

- **Conducting joint trainings with foreign partners.** For example, in the period 11-22 January 2016, a joint training exercise "BLACK SEA ROTATIONAL FORCE 15.2" – PLATINUM LION 16-2, Land Ops" was held at the Novo Selo Training Range. It was attended by personnel from the US Marine Corps, units from the Land Forces of the Republic of Bulgaria, cadets and teachers from the NMU "V. Levski", units from Romania, Hungary and Croatia. Participation in such international exercises contributes to the exchange of experience and standardization of procedures between the participants.

The application of these approaches outlines a number of advantages and challenges regarding the integration of theoretical and practical training. The advantages that can be mentioned are: better knowledge acquisition, development of problem-solving skills, increased motivation, better preparation for professional activity. As challenges, first of all, we can highlight resource provision. Without the necessary equipment, ranges and instructors, it is impossible to apply theoretical knowledge in practice. Next is ensuring safe conditions for conducting practical classes. And last but not least, it is finding a balance between theory and practice.

The integration of theoretical and practical training is a key factor for the success of modern military education in Bulgaria. It allows for the preparation of highly qualified specialists capable of responding to modern challenges to national security. In order to achieve full integration, it is necessary to overcome existing challenges and continue the development of existing models.

2.3. Integration of different types of training

Individual training focuses on the development of specific skills and knowledge of each learner. It allows for a personalized approach, deeper understanding of the material, and the development of self-discipline and responsibility.

The collective training emphasizes the importance of interaction and cooperation between learners. It develops communication skills, teamwork, leadership qualities, and social skills.

Individual and collective training are two fundamental approaches in the educational process, which complement each other and play a major role in the development of military specialists. Their integration within military education aims to achieve a balance between the development of individual skills and effective interaction to achieve optimal results and build effective teams.

Traditional methods and forms of training in military education are based on strict discipline, hierarchical structure and an emphasis on the development of basic military skills. They are described in the Training Doctrine, contained in the training methodologies for the relevant disciplines and include lectures, exercises, practical classes, etc.

Innovative methods and forms of training are a new approach in military education, using modern technologies and interactive teaching methods. These can be simulations, virtual and augmented reality, mobile applications, online learning, etc.

From the perspective of the integration of these methods and forms, NP-7 states that the choice of the most appropriate training methods is important for the overall functioning of the system. [7, p. 13]. In addition, the doctrine allows teachers and instructors to be creative in their use, stating that the forms of training are open, i.e. they can be complemented, intertwined and combined, aiming to achieve the maximum effect of their use [7, p. 60].

Successful integration of traditional and innovative methods and forms of training requires a balanced approach and adaptive planning. To achieve the training objectives, various integration models can be used, such as:

- combining methods and forms;

- personalizing training;

- focusing on the development of problem-solving and critical thinking skills;

- stimulating learners to analyze situations, make decisions and act in non-standard conditions;

- constantly evaluating the effectiveness of training.

IV. Conclusions

The analysis of integration processes in the military education system reveals the central role of comprehensive and adaptive strategies for bringing military education into line with contemporary societal, technological, and operational requirements. The study highlights the importance of promoting synergy between civilian and military educational components, integrating theoretical knowledge with practical training, and adopting innovative teaching methodologies and technologies. These efforts are essential to equip military personnel with the skills and competencies needed to effectively address evolving national and international security challenges.

In conclusion, integrating different educational approaches is crucial to increasing the effectiveness of military education. Future efforts should focus on:

1. Strengthening cooperation. Promoting partnerships between military academies, civilian universities, and research organizations by developing joint programs, sharing experiences, and conducting joint research will enhance the exchange of knowledge and resources and ensure that curricula are aligned with global trends in education and security.

2. Adapting to change. The evolving nature of security threats and technological advances require continuous updating of educational programs, which will ensure that graduates of higher military schools will possess the necessary knowledge, skills and competencies.

3. Emphasis on practical experience. Increasing opportunities for practical training and simulations that reflect real-world scenarios will allow learners to apply theoretical knowledge in practical settings.

4. Investing in resources. Although listed last, this is one of the most important areas for development, requiring the provision of adequate funding and resources for training facilities, equipment and teacher development to support high-quality education.

By implementing these suggestions, military education systems can better prepare their graduates for the complexities of the modern defense and security environment.

REFERENCES

[1] S. Ilieva, “The integrated approach in the training to increase the effectiveness of the learning process,” In Proceedings of University of Ruse “May Research Conference”, 2017, vol. 56, book 11, pp. 111-116. [in Bulgarian]. Available: https://conf.uni-ruse.bg/bg/docs/cp17/11/11-19.pdf. [Accessed December 02, 2024].

[2] M. Andreev, *The Learning Process. Didactics.* Sofia: University Publishing House “St. Kliment Ohridski”, 1996. [in Bulgarian].

[3] National Assembly, *Strategy for the Development of Higher Education in the Republic of Bulgaria for the Period 2021 – 2030*. Sofia: National Assembly, Promulgated in the State Gazette, No. 2 of January 8, 2021. [in Bulgarian]. Available: https://dv.parliament.bg/DVWeb/showMaterialDV.jsp?idMat=154629. [Accessed December 11, 2024].

[4] Vasil Levski National Military University, *Strategy of the Vasil Levski National Military University 2030*. Veliko Tarnovo: Vasil Levski National Military University, 2023. [in Bulgarian]. Available: https://www.nvu.bg/sites/default/files/2023-07/strat_2030_nvu.pdf. [Accessed December 10, 2024].

[5] Rakovski National Defence College, *Development Strategy of Rakovski National Defence College 2021-2030*. Sofia: Rakovski National Defence College, 2021. [in Bulgarian]. Available:

https://rndc.bg/wp-content/uploads/2023/03/%D0%A1%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D0%B8%D1%8F-%D0%B7%D0%B0-%D1%80%D0%B0%D0%B7%D0%B2%D0%B8%D1%82%D0%B8%D0%B5-%D0%BD%D0%B0-%D0%92%D0%90-2030.pdf. [Accessed December 10, 2024].

[6] D. Berchev and M. Stefanov, "The Systems Approach to Training in the Military Educational System – aggregation of integration processes," *KNOWLEDGE – International Journal*, vol. 30, no. 6, March, pp. 1457-1462, 2019. Available: https://ikm.mk/ojs/index.php/kij/article/view/1620/1619. [Accessed December 12, 2024].

[7] Ministry of Defense, *Doctrine for training the armed forces of the Republic of Bulgaria.* (National publication of the Armed Forces of the Republic of Bulgaria NP-7, Edition A). Sofia: Ministry of Defense, 2018. [in Bulgarian].

[8] D. H. Schunk, *Learning Theories an Educational Perspective*, 6th ed. Boston, MA: Pearson, 2012. Available: https://elmirmohammedmemorypsy.com/wp-content/uploads/2017/11/learning-theories-an-educational-perspective.pdf. [Accessed December 08, 2024].

[9] I. Dechkova, "Educational Systems Around the World – part 1," *The magic of art-word, music and dance*, August 8, 2023. [Online]. Available: https://magicart-delta.com/en/2023/08/08/%d0%be%d0%b1%d1%80%d0%b0%d0%b7%d0%be%d0%b2%d0%b0%d1%82%d0%b5%d0%bb%d0%bd%d0%b8%d1%82%d0%b5-%d1%81%d0%b8%d1%81%d1%82%d0%b5%d0%bc%d0%b8-%d0%bf%d0%be-%d1%81%d0%b2%d0%b5%d1%82%d0%b0-%d1%87%d0%b0%d1%81/. [Accessed December 14, 2024].

[10] I. Dechkova, "Educational Systems Around the World – part 2," *The magic of art-word, music and dance*, August 8, 2023. [Online]. Available: https://magicart-delta.com/en/2023/08/08/%D0%BE%D0%B1%D1%80%D0%B0%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D0%BD%D0%B8%D1%82%D0%B5-%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B8-%D0%BF%D0%BE-%D1%81%D0%B2%D0%B5%D1%82%D0%B0-%D1%87%D0%B0/. [Accessed December 14, 2024].

[11] D. Markov and R. Chalakov, *Challenges Facing the Development of the Military Education System*. Sofia: Rakovski National Defence College, 2023. ISBN: 978-619-77-11-21-9. [in Bulgarian].

[12] K. Kalinov, "Modern Education – What Everyone Understands," *Security and Defense*, issue 1, pp. 85-95, November, 2022. [in Bulgarian]. [Online serial]. Available: https://doi.org/10.70265/VCEN6523. [Accessed December 15, 2024].

[13] National Assembly, *Law on Defense and Armed Forces of the Republic of Bulgaria*. Sofia: National Assembly, Promulgated in the State Gazette, No. 35 of May 12, 2009. [in Bulgarian]. Available: https://lex.bg/laws/ldoc/2135631954. [Accessed December 16, 2024].

[14] Council of Ministers, *Regulation on the state requirements for acquiring higher education at the educational-qualification degree "bachelor" in the professional direction "Military Affairs" in the specialties of the regulated profession "Tactical level management officer"*. Sofia: Council of Ministers, Promulgated in the State Gazette, No. 68 of September 4, 2012. [in Bulgarian]. Available: https://lex.bg/laws/ldoc/2135808720. [Accessed December 16, 2024].

[15] D. Berchev and S. Petkov, "Integrating Simulation Systems in Cadet Training: Challenges and Opportunities," In Proceedings of the Second National Scientific-Practical Conference "Digital Transformation of Education – Problems and Solutions," 2024, pp. 320-324. [in Bulgarian]. Available: https://www.conf-dte.bg/docs/2024/p-57.pdf. [Accessed December 16, 2024].

[16] Institute for Defense and Business (IDB), "The Experiential Learning Model (ELM) in the Military," *Institute for Defense and Business (IDB)*, 2024. [Online]. Available: https://www.idb.org/the-experiential-learning-model-elm-in-the-military/. [Accessed: December 12, 2024].

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 285-289

Globalization and Global Security

Nikolay Penchev Stefanov
Vasil Levski National Military
University, Veliko Tarnovo, Bulgaria
Veliko Tarnovo, Bulgaria
niki.s@abv.bg

***Abstract*—The concept of "global security" is a fundamental category in the theory of international relations and foreign policy practice. In the face of constantly changing asymmetric risks and threats to the national security of countries, the need to create a collective security system is growing. National security is directly related to international or more precisely global security. Above all, the global security environment is characterized by a rise in non-state and international threats to national security. This article examines the goals, objectives and elements of globalization and global security. The study argues that there cannot be a global security system in which there are no risks and threats to the international community, states and individuals.**

Keywords— globalization, global security, global security system, international security, national security.

I. Introduction

The modern security environment and dynamic changes on a global scale require the use of alternative and modern methods for ensuring national security [8].

National security is a state of the state, the individual and society that changes its essence, in which all important and significant interests for their normal existence, prosperity and development are protected.

It is a set of measures through which the state guarantees the well-being of the individual and society. It includes the prevention of threats, both internal and external, to the protection and well-being of citizens.

II. Materials And Methods

This study covers scientific research methods, such as:

- indirect observation method – through the study of theoretical sources, publications, regulatory acts and organizational documents, economic and legal analysis for their processing and interpretation;
- a method of retrospection and forecasting to examine the past state and predict future development trends of the problem;
- methods of scientific knowledge, such as theoretical, comparative and factor analysis, as well as generalizations and conclusions based on data from the researched and used sources of information.

III. Results and Discussion

The increasing international economic integration, known as "globalization", offers many opportunities. The concept of globalization is increasingly being studied, given its relevance. This so-called process is undoubtedly associated with the word development - borders are open, the Internet allows us to learn everything we need in a second, national markets are open, etc. It offers a number of opportunities. Despite the positive trends outlined by the pace of development of globalization, its existence also triggers negative phenomena, such as international terrorism, cross-border organized crime, the spread of weapons of mass destruction, energy security problems, etc [9]. According to Jean-Marie Guéhenno, one of the most important strategic consequences of globalization is that it changes the nature of threats [6].

Globalization is related to the development of international trade and the global distribution of goods and services, through the reduction of barriers to international trade, such as customs tariffs, export taxes and import quotas, as well as restrictions on the movement of capital and investment. One of the most common views about the consequences of the globalization process is that economic growth and new information technologies will lead, almost automatically, to a new era of global understanding and political stability [7]. The impact of various aspects of globalization (economic, political, cultural, demographic, religious, etc.) on security can be both positive and destructive [6].

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8507
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

A number of researchers believe that globalization is the process of increasing political, social, economic, technical and cultural interconnections and relationships between individual countries, organizations and people.

This process gives rise to rapid and effective changes in social relations, which in turn predetermine the manifestations of various forms of confrontation or cooperation in international relations. Nowadays, globalization is a major factor determining the directions and pace of national, regional and global development. However, thanks to it, new and new risks and threats appear. On the other hand, it is precisely it that helps to strengthen the security of states. Therefore, global security as a concept is inextricably linked to globalization, and it, in turn, is connected with the goals and objectives of the global security system.

Today, the goals and objectives of the global security system are impossible to resolve outside the global space.

A. Meaning of the category "global security"

The term "global security" or "international security" expresses a basic category widely used both in the study of international relations and in the implementation of international policy.

In implementing a global security policy, it is necessary to achieve a high level of counteraction to asymmetric risks, dangers and threats [5].

The state of security on the global stage can be determined by the presence of several basic elements that drive the global security system.

Maintaining the system of global relations in a state of security and stability depends not only on the effective counteraction to risks and threats of various nature, but also on the creation of conditions for its long-term stability, which is associated with other important elements.

A fundamental element of the global security system is the implementation of a high level of stability and security of international relations and international order, the degree of professionalism in following the norms of international law, the implementation of close ties and interaction between states on a global scale, under conditions of mutual understanding, peace and cooperation [1].

The second important element is the implementation of international policy at the global level under conditions of a high level of caution and predictability regarding the behavior of individual states. This implies clarity, openness and publicity.

It should be noted that a state of complete predictability cannot exist due to the constant change of risks and threats to the security of countries, i.e. some factors disappear on the international scene, others appear. However, the lack of predictability increases the risk factor far beyond reasonable limits, and this in itself leads to uncertainty.

The third element that is necessary to guarantee global security, and hence the security of an individual state, is the creation of an environment in which there are no intertwined interests, which implies lowering the threshold of possible factors that can provoke conflicts leading to sharp contradictions, threatening world peace and "increasing the force factor" [1].

A fourth important element of the global security system is the creation of an organized structure of international bodies and organizations that can effectively confront existing and growing risks, dangers and threats on the international scene. These bodies and organizations should work in close connection and cooperation with other state organizations at the national level.

If these four main elements are combined, an approximate working definition of the category of "global security" can be given as: A state of relations between states on the global stage, in which a high level of peace, security and cooperation is achieved and effective counteraction to existing risks, dangers and threats is achieved, under conditions of a high degree of predictability, clarity and understanding, and if risks and threats nevertheless appear, there are sufficient grounds that they can be easily reduced, parried or overcome.

Based on the analysis of the constructed definition, it can be concluded that global security contains two aspects of manifestation. On the one hand, it guarantees the security of all states participating in international relations, on the basis of established and existing norms and rules of international law, i.e. of the world as a whole. On the other hand, global security is a guarantor of the stability, independence, sovereignty, prosperity and territorial integrity of each individual state participating in international relations, by guaranteeing the rights, freedoms, protection of vital interests and well-being of the individual and society, i.e. it is a factor for the proper functioning of the lower levels of security - national, group and individual.

It should be noted that in international relations, too, a state of absolute security cannot exist due to the constantly changing asymmetric risks and threats to security. Therefore, global security is called upon to maintain an optimal level of protection of vital interests, in order to guarantee peace, stability and prosperity of states on the world stage, with all available forces and means.

The significance of the category of "global security" is emphasized by the fact that it includes an extremely voluminous content. This applies even to the category of "security" alone".

Security is a basic category and an inherent human value. It is a basic human need and a primary factor for the existence of prosperity and development. Global security is the first, highest level of security. Placing it at the top of the hierarchy also assigns the important importance of guaranteeing the vital interests of the individual state, individual and society. That is why ensuring peace, understanding and cooperation in building foreign policy is "the highest good and the main goal of every state" [3]. In addition to everything else, peace, stability and security

are not only a goal, but also an inherent and inalienable right, guaranteed by the norms of international law.

The pursuit of security and protection is a conscious need, a value and a basic need to which we all strive. Its guarantee is not only an interest, but also an obligation of all those persons, bodies and organizations that are called to protect it. This is where the deepest essence of the concept is rooted. It is a right that no individual can be deprived of.

The strengthening of security protection in all directions and on the territory of all countries around the world is of paramount importance both for international policy and for the national policy of each state. Attempts to destroy peace, unanimity and cooperation, as well as to undermine security on the territory of a given country, region or continent by force are sufficient grounds for decisive countermeasures both at the national and global levels.

Nowadays, the international situation and the way international relations develop create the necessary prerequisites and guidelines for choosing options for action when building a foreign policy strategy of an individual state. International law proclaims security, stability, understanding, cooperation and the resolution of conflicts peacefully, through soft power and means as the highest criteria for making foreign policy decisions. The choice is predetermined by the norms of international law.

Today, every state realizes that the establishment of the principles of peace and security, in relation to constantly changing risks and threats, is impossible in conditions of isolation.

In the modern world, globalization sets the pace of development of the state and society. The changes taking place on a global scale require coordinated interaction and cooperation on the international stage to achieve lasting peace and stability.

The ways to achieve an optimal level of security require the correct determination of the "most likely and preferred scenarios for the development of the global security system in the long term" [4]. Therefore, maintaining the stability and security of states and the world is impossible without the process called globalization.

Globalization invariably accompanies the processes of change and development of states and outlines the necessary ways, methods and means of developing foreign policy. For this reason, the global security system is inextricably linked and cannot exist separately from globalization.

B. Purpose and tasks of globalization and global security

Globalization is a process of deepening and convergence of the processes of interaction in the economy, politics, culture, education, social activities, information development, etc. between individual states in the global space "in the direction of transforming the purpose of state-territorial borders" [1]. It is associated with a number of turbulent universal changes that impose their positive and negative trends on the development of the individual state. The role played by global security is to manage these changes, modeling them in a way that allows achieving an optimal level of security and stability in relations between states in the international space. On the other hand, the process of managing these changes is possible thanks to the globalization process.

In summary, four main influences of globalization processes on the debate on global security can be identified:

- in terms of the dynamically changing international situation;
- in terms of the domestic policy and foreign policy orientation of the state in the field of security;
- in terms of determining the ways to achieve security.
- in terms of understanding the role of international security [1].

As for the dynamically changing international situation, one of the most discussed concepts is precisely change. The constant change of the security environment, caused by asymmetric dangers, risks and threats, leads to the need for continuous restructuring and conceptualization of strategies for overcoming uncertainties. Thus, the problem of change management becomes a current need today.

Today, the need to build a system of modern ways and methods for protecting both the security of individual states and international security is brought to the fore. This system should be adequate to the continuous restructuring of the challenges, dangers and threats accompanying development.

The need to build effective ways and means through which "to overcome potentially emerging or existing dangers to the vital interests of the countries participating in international relations" [4] comes to the fore.

In terms of the internal policy of states in the field of security, it should be borne in mind that the democratic tradition in itself guarantees the affirmation of the protection of the rights, freedoms and vital interests of the individual and society as supreme values. This corresponds to the understanding of security as a supreme good, which is called upon to ensure their realization.

In terms of the foreign policy orientation of states in the field of security, it should be noted that after the devastating upheavals that humanity experienced in the 20th century, as well as in connection with newly emerging threats to security, states felt the need to maintain lasting peace. In the name of achieving this peace, they partially gave up their sovereignty, in the name of higher goals. Individual countries realized that the spread of new threats and risks to humanity, such as terrorism, international organized crime, trafficking in people, weapons and drugs, the spread of weapons of mass

destruction and wars, have a transnational character. No country is capable of dealing with these factors with its own forces and means.

In recent years, the understanding of the ways to achieve security and stability has also changed significantly. The bitter experience of the two world wars in the twentieth century has forced countries to rethink the forms of action to ensure security. In the current century, the force factor is giving way to the so-called "soft power", characterized by the imposition of sanctions that are not of a military nature - economic, financial, environmental, demographic, informational, cultural and others [3].

In terms of understanding the role of international security, the reasons for the development of the global security system, its essence, as well as the goals and objectives that it sets for itself are important.

In the fight against constantly transforming risks, dangers and threats of a global nature, countries are aware of the need for mutual understanding and cooperation.

C. Purpose and tasks of the global security system

The main goal of the global security system is to counteract the asymmetric risks and threats that are generated, on the one hand, by the processes of globalization, and on the other hand, by the policies of individual states.

One of the main tasks of the global security system is the rejection of aggression as a policy for protecting interests and resolving disputes between states. In our era, for the first time in the history of nations, there is a real opportunity to eliminate war as a means of defense. States are increasingly realizing that war as a means of defending interests always brings more destruction than benefits. Thus, they are reorienting themselves to softer methods, such as negotiations, etc. The modern international situation seeks to establish the principles of peaceful coexistence in relations between states.

Another main task of the global security system is to build security against an unstable economy and prevent the gap between the rich and the poor from widening. The problem is that world wealth is distributed very unevenly. According to statistics, only 22% of world wealth belongs to developing countries, where, ironically, 80% of the population lives. This uneven distribution leads to a number of problems caused by social discontent. Thus, the tasks of the global security system are added to resolve such as: countering international terrorism, countering international organized crime, reducing illegal migration, countering trafficking in people, weapons and drugs, countering the proliferation of weapons of mass destruction, preventing ethnic and religious enmity, preserving the rights and freedoms of citizens, preserving the rights of peoples to self-determination, etc. Another main task is to prevent threats to environmental security. As a result, various global strategies have been created to limit the harmful effects of human activity, uniting dozens of countries.

IV. CONCLUSIONS

The global security system is a dynamic system that characterizes the state of external relations of countries participating in international communication, in which there are no risks and threats to the vital interests of individual countries and the international community, and in the event that such threats nevertheless arise, there are reliable ways and means to overcome them so that the normal functioning of the system and the normal development of each country are not damaged.

On the one hand, it embodies the security of the international community or the world as a whole, and on the other hand, it embodies the security of individual countries - national security. National security is a dynamic state of the state and society, in which the fundamental rights and freedoms of citizens and the sovereignty, independence and territorial integrity of the state are protected. Based on these statements, it can be concluded that global security, the security of the world, is the foundation on which the security of the following subjects (levels) is built: security of the region, security of the state, security of society, security of the individual.

A state of complete security cannot exist, nor can a full assessment of the dangers, risks and threats that may arise in this sphere be made. In this sense, there cannot be a global security system in which there are no risks and threats to the international community, states and individuals. Therefore, the purpose of the global system is to promptly detect, assess and neutralize risks and threats to individuals and their communities, to the state, the region and the world.

Protecting security requires not only identifying and countering risks and threats, but also creating conditions for its long-term stability. This process would be impossible without the development of globalization, on the one hand, as well as without the established international security and cooperation organizations that are part of the global security system.

ACKNOWLEDGMENTS

This report is supported by the National Scientific Program "Security and Defense", approved by Decision No. 171/21.10.2021 of the Council of Ministers of the Republic of Bulgaria.

REFERENCES

[1] B. Alexandrova, “Globalization and International Relations.”, ISBN 9789540740928, Publisher: St. Kliment Ohridski University, 2016.

[2] D. Bratanov, "Peace and the Responsibility of Nations", Monograph, Sofia, Publisher: Partizdat, 164 p..

[3] G. Stefanov G, “Theory of International Relations”, ISBN: 978-954-64-9081-0, Publisher: Ciela, 2007.

[4] N. Dolchinkov, “Results and Analysis of Achieved Joint Research and Activities Between Rezekne Academy of Technology and Vasil Levski National Military University”, 14th International Scienfic and Practical conference Environment. Technology. Resources. Vide. Tehnologija. Resursi, 2023, ISSN 1691-5402, 3, pp. 90–93.

[5] J. M. Guehenno, "The Impact of Globalization on Strategy.- Survival", N 4, Winter, 1998-1999.

[6] G. Kresnaliiska and O. Chorbadzhiyska, "Impact of globalization and regionalization on governance in the public sphere", Yearbook of the Department of „Administration and Management", 2017, pp. 21–27.

[7] N. Nichev and K. Koynakov, "Use of Unmanned Aircraft in the Logistics Support of Military Formations", The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM) ISSN: 2602-3199, Volume 31, Pages 92-99.

[8] A. Andonov, "From total war to considerations of collateral losses. Historical aspects of joint targeting", International Scientific Conference "110 years of tradition, quality, prestige", 12–13.04.2022, Military Academy "Georgi S. Rakovski", Sofia, ISBN 978-619-7478-88-4, pp. 40-45

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 291-296

Conceptual Convergence: Disinformation, Fake News, and Information Influence as a Triad of Security Threats in the Context of Society 5.0

Dimitrina Stefanova
Department "Public Relations"
South-West University "Neofit Rilski"
Blagoevgrad; Bulgaria
d.stefanova.swu@gmail.com

Kristiana Bacheva
Department of Library Science
University of Library Studies and Information Technologies, Sofia, Bulgaria
christiana.stefanova05@gmail.com

Valentin Vasilev
Head of "Center for Leadership and Public Policies"
Higher School of Security and economics
Plovdiv, Bulgaria
valentin.vasilev@vusi.bg

***Abstract*— The rapid advancement of technologies and the widespread application of communication tools significantly transform how individuals perceive and interact with information. Concurrently, the increasing volume of data and the sophistication of information technologies necessitate robust conceptual frameworks to ensure information security. This shift underscores the evolution of information into a critical and valuable resource, making it a prime target for influence in both business and societal contexts. Disinformation, fake news, and information influence have emerged as tools of interference, posing severe threats to modern societies. These phenomena can undermine democratic institutions and processes by obstructing individuals' ability to make informed decisions regarding their professional, social, and public lives. In recent decades, their role as threats has become integral to the evolving paradigm of security. In the dynamic context of the contemporary world, the traditional understanding of "security" has gradually expanded to encompass a broader, interdisciplinary approach. This new perspective incorporates economic, informational, environmental, social, and technological dimensions, redefining security as a complex phenomenon requiring adaptive and comprehensive solutions. The scientific and applied research into disinformation, fake news, and information influence, as subversive processes, is multifaceted and spans various disciplines. In the security domain, these phenomena are defined and analyzed within strategic and normative frameworks. This paper aims to conduct a documentary review and analysis of the conceptual apparatus employed in national strategic and normative documents through the method of content analysis. Focusing on their application to countering information threats, the study will interpret and evaluate these concepts. The proposed approach seeks to establish conceptual convergence and develop a sustainable framework to address these challenges effectively.**

Keywords –Disinformation, Fake News, Information Influence, Security.

I. INTRODUCTION

In the context of security, it can be observed that the current digital era is bringing about profound transformations across all areas of society.

The Fifth Industrial Revolution presents both challenges and opportunities, driven by the collaboration between humans and artificial intelligence, which is reshaping work, innovation, and daily life. However, without a global consensus on technology governance and best practices, risks such as data breaches, misinformation, mass surveillance, and personal data threats will persist. Additionally, unregulated advancements in automated and immersive technologies may introduce unforeseen risks.

Technological innovations, alongside political and social changes, create not only new opportunities but also significant risks. In addition to traditional threats, emerging hazards such as cyberterrorism, communication-based violence, disinformation, fake news, disruptions to critical infrastructure, manipulations via genetic engineering, and the effects of climate change are increasingly interwoven with conventional risks, evolving into hybrid crises. These processes stimulate debates within the public and business sectors, as well as among the media and civil society, because despite the many positive aspects, the information age introduces unique

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8470
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

threats that substantially impact the security of organizations and society as a whole.

The balance between innovation and regulation is crucial for ensuring information security and promoting progress. Establishing expert capacity to detect fake news, disinformation, and provocative content is an important task that requires an interdisciplinary approach. It is essential to develop policies for effective counteraction, considering that digital processes must be examined within two interconnected dimensions—technological and social. The way in which new technologies intertwine with social relations fundamentally transforms the models of interaction among actors and influences both systems and their defenses. This necessitates a cautious perspective on the exponential increase in the volume, speed, and quality of information, as well as the new requirements for securing the informational environment and its participants. Consequently, there is a pressing need to establish a national management system that protects not only the information and the informational environment but also the human factor within it.

II.Materials and methods

The methods employed in this study include theoretical analysis, deductive reasoning, and content analysis of literary sources and national-level strategic documents. In a comparative perspective, European policies and practices for combating deliberately manipulated information and its impact have also been examined.

III. Results and Discussion

Information is now the most significant and contested geopolitical resource in the world. The most profitable businesses have long claimed that data is “the new oil.” Data and innovation not only transform economies and societies but also reshape international relations. The pursuit of informational power compels states to reconsider their interactions with markets and citizens by rewriting their national interests and strategic priorities. This fundamental transformation in the role and behavior of the state can have serious, even seismic, consequences. In particular, authoritarian regimes, recognizing the strategic importance of information, have, over the past five years, implemented powerful domestic and international informational strategies—isolating their information environments from global flows and using information as a tool for attacking and destabilizing democracies [1].

Defining the key concepts and principles is of paramount importance for the development of any scientific discipline and practice. The vision for converging the concepts of “disinformation,” “fake news,” and “information influence” involves extracting their common characteristics, as well as considering them in the context of ensuring security from the perspective of the state as a primary priority and obligation to protect its interests. This vision comprises three core components - security, influence, and information - with security playing a regulatory role over the latter two. Hundreds, if not more, of the current studies dedicated to “disinformation,” “fake news,” and “information influence” attest to the fact that these topics belong to a multidisciplinary field that combines scientific research and professional practice in developing and implementing countermeasures. The goal is to strike a balance between these elements in order to guarantee the planet's and humanity's long-term prosperity [2].

Among the unifying definitions, for instance, Wardle (2017) defines disinformation as “the deliberate creation and dissemination of false or misleading information with the intent to deceive or manipulate public opinion” The topics of mis-, mal- and disinformation are too important to start legislating and regulating around until we have a shared understanding of what we mean by these terms [3]. Disinformation refers to information that is deliberately false and is disseminated with the purpose of deceiving its audience, manipulating beliefs, and harming its target.

False and misleading information in its varying forms may lead to increasing misperceptions and knowledge resistance, which in turn pose significant threats to the health and well-being of individuals as well as organizations, countries, democratic deliberation and democracy per se [4]. Gelfert (2018) discusses disinformation in a similar context:” The term ‘disinformation’, more so than the relatively recent expression ‘fake news’, has by now received considerable attention from epistemologists and has been subjected to extensive conceptual analysis [5]. Fake news is best defined as the deliberate presentation of (typically) false or misleading claims as news, where the claims are misleading by design. The phrase “by design” is then explicated in terms of systemic features of the process of news production and dissemination.

All these definitions emphasize that disinformation constitutes deliberately crafted and disseminated false or misleading information, aimed at deceiving or manipulating the audience. The common elements are:

Intent: The information is produced with a pre-determined objective in mind.

Falsehood/Misleading Nature: The information is defined as false, untrue, or distorted in a manner that misleads the recipient.

Manipulation: The primary aim is to manipulate the beliefs, opinions, or actions of the audience, which may be pursued for political or financial purposes.

In related research, Tandoc Jr. et al. (2018) define fake news as “news content that mimics the format and style of legitimate journalism but is deliberately fabricated or manipulated, containing false information intended to mislead its audience” [6].

Petko Dimov and Elislav Ivanov argue that "fake news is a neologism, often used to refer to unwanted pseudo-news or propaganda aimed at deliberate disinformation or the generation of revenue through online advertising. The dissemination of fake news constitutes 'informational pollution,' which significantly intensifies during elections" [7].

These definitions underscore the intentional nature of both disinformation and fake news, highlighting their roles in purposefully deceiving and manipulating audiences, with fake news being viewed as one of the forms through which disinformation manifests in the media sphere.

Drawing on longstanding practices, the European Union, through its institutions, proactively develops policies, methodologies, analyses, and responses related to disinformation instruments aimed at the tactical and strategic manipulation of phenomena and processes associated with informational and national security. The European Parliament defines "fake news" and disinformation as information that is deliberately manipulated with the intent to deceive people, and which is emerging as an increasingly prominent global phenomenon [8].

At its level, The European External Action Service (EEAS), which is the EU's diplomatic service, defines a process of Foreign Information Manipulation and Interference (FIMI) - also often labeled as "disinformation" - is a growing political and security challenge for the European Union.

„Defining FIMI: The EEAS defines FIMI as a pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory.

This first edition of the EEAS report on Foreign Information Manipulation and Interference (FIMI) threats is informed by the work of the European External Action Service's (EEAS) Stratcom division in 2022. Based on a first sample of specific FIMI cases, it outlines how building on shared taxonomies and standards can fuel our collective understanding of the threat and help inform appropriate countermeasures in the short to the long term" [9].

Definition of FIMI: The European External Action Service (EEAS) defines FIMI as a behavioral model that threatens or has the potential to negatively affect values, procedures, and political processes. Such activities are characterized by their manipulative nature and are carried out deliberately and in a coordinated manner. Participants in these activities may be state or non-state actors, including their proxies both within and outside their own territory.

Context and Need for a Comprehensive Counteraction Framework: In the context of informational attacks and the deliberate, coordinated activities of "manipulation and interference of foreign information" (FIMI) aimed at exerting a negative influence on political and social processes and values, a comprehensive counteraction framework is required. This framework should encompass rules, theories, methods, and practical implementation approaches. Within this semantic framework, disinformation, fake news, and information influence are not only seen as communication phenomena but also as serious threats to national and global security. Implementing such an approach necessitates integrated efforts at technological, legal, and social levels to ensure stability and protection in the digital age.

European Commission Report on Online Disinformation: The European Commission's first report, titled Tackling online disinformation: a European Approach (published in 2018), underscores the Commission's strong resolve to combat all forms of disinformation, which underpin various types of fake news. The report "Disinformation is understood as verifiably false or misleading information that is created, presented, and disseminated for the purpose of economic gain or deliberately to mislead the public, and that may cause public harm. Public harm includes threats to democratic political processes and policy-making, as well as to public goods such as the protection of the health of EU citizens, the environment, or security."

At the same time, large-scale online disinformation campaigns are widely employed by a range of local and foreign actors to sow distrust and generate social tension, with serious potential consequences for security. Furthermore, disinformation campaigns orchestrated by third countries can be part of hybrid threats to internal security, including during electoral processes, especially when combined with cyberattacks. Measures to protect citizens from the destructive effects of misinformation at the European level highlight the necessity for coordinated actions across multiple domains [10].

Overall, these definitions emphasize the deliberate dissemination of false information with the aim of manipulating and undermining democratic processes, by strategically using information as a tool of influence. It is also a key instrument in human capital management within organizations [11].

Disinformation is intentionally manipulated information that misleads the audience, often referred to as "fake news." It is considered a form of "informational pollution," which becomes particularly pronounced during elections. The European Union is actively developing policies and methodologies to address these phenomena, which pose challenges to societal security by manipulating information and interfering with political processes.

From a security perspective, the reviewed publications highlight several key aspects:

Deliberate Deception: Disinformation is characterized as deliberately created, manipulated, and disseminated information intended to deceive or manipulate public opinion, an occurrence often labeled as "fake news" or informational pollution, especially noticeable during elections.

Strategic and Tactical Information Influence: Information influence manifests through strategic and tactical processes that manipulate informational flows to alter political, social, and economic processes.

Threat to National and International Security: Both the European Parliament and the European External Action Service (EEAS) define these phenomena as tools for manipulating values, procedures, and political processes, posing a serious threat to both national and international security.

Objective of Manipulation: Disinformation and information influence are aimed at deliberately deceiving the audience by altering perceptions and behaviors in favor of specific political, economic, or ideological objectives.

Undermining Public Trust: Disinformation can erode trust in state institutions, the media, and the judicial system, leading to destabilization and vulnerability in national security, thus creating an environment conducive to both internal and external manipulations.

Role of Digital Platforms: European documents stress the significance of digital platforms and algorithms in disseminating disinformation. This highlights the necessity for enhanced cybersecurity measures, increased algorithmic transparency, and improved monitoring of online content to prevent the rapid spread of fake news.

Hybrid Warfare Instrument: Disinformation is regarded as an instrument in hybrid warfare, utilized to manipulate public opinion and destabilize political and social structures. Such multifaceted attacks present significant challenges to national security, as they are complex and difficult to localize.

It should be noted that "disinformation," in all its forms and modes of dissemination, is a transnational problem that necessitates a coordinated approach among states. Common strategies and the exchange of information are key to effectively protecting democratic institutions against manipulation.

In this context, a pertinent yet critical question arises: can individuals, groups, organizations, and/or societies fall into an "information catastrophe" due to informational pollution? Just like that, many global experts have reached the conclusion that if pollution continues at the same rate, in 30 years the oceans may contain more waste than living matter, an outcome tantamount to an ecological catastrophe [12].

As an EU member, Bulgaria has undertaken commitments related to international conventions and EU legislation, which form the foundation for the development of national security law. The present study examines the necessity of establishing expert capacity to ensure security against manipulative informational influence, with such capacity needing to be institutionalized within the country's strategic and regulatory documents. According to the Law on Strategic Planning of the Republic of Bulgaria, the National Strategic Framework represents an integrated system of strategic documents (e.g., the National Development Program, National Strategy, Roadmap, and Action Plan) that defines national priorities and the means to achieve them [13].

Within the scope of this study, a content analysis was conducted on two key strategic documents selected based on expert criteria. The defined units of analysis are the key concepts: disinformation, fake news, and information influence, including an in-depth qualitative analysis of their meanings and interrelationships in the context of hybrid actions.

The Updated National Security Strategy of the Republic of Bulgaria (2018) emphasizes the growing threats associated with hybrid actions, which include targeted manipulations by state and non-state actors, organized criminal groups, and terrorist organizations. Particular attention is given to the exploitation of cyberspace to propagate radical ideas, manipulate public opinion, and disseminate disinformation [14].

In the Updated National Cybersecurity Strategy "Cyber Resilient Bulgaria 2023," different levels of threat awareness are defined (ranging from "known-knowns" to "known-unknowns"), emphasizing the complexity of modern cyber threats, including disinformation campaigns [15]. The document outlines factual tools within a hybrid warfare model, which integrates both conventional and unconventional actions, including cyberattacks, psychological and economic influence, and disinformation campaigns, aimed at achieving political and strategic objectives. It recognizes the uniqueness of each hybrid strategy, highlighting the necessity for responses to be tailored to its specific characteristics. The strategy underscores the importance of engaging all relevant stakeholders—government, the private sector, education, NGOs, media, and civil society—to enhance cyber culture and effectively manage cyber risks. The forms and methods of human growth and self-expression are important. "Culture, unlike the unifying effect of globalization, differentiates different communities" [16].

The integration of expert capacity for countering manipulative informational influence into strategic documents is crucial for national security. The results of the content analysis of current national security and cybersecurity strategies indicate that information manipulation tools are incorporated rather peripherally and primarily in the context of hybrid threats.

CONCLUSIONS

With a growing awareness of sustainable The systematic definition of seemingly homogeneous concepts—disinformation, fake news, and informational influence as subversive processes—within strategic security documents would offer several key benefits for ensuring institutional, organizational, societal, and national security. „Disinformation, or fake news, consists of false or misleading information that is created, presented, and disseminated for political or economic gain or to deliberately deceive the public, causing social harm. Today, this phenomenon has a greater impact than ever, as it has become easier for anyone to publish and share news or information online. Social media and online platforms play a crucial role in accelerating the spread of such news, enabling a global reach with minimal effort from the author" [17].

Successfully addressing the challenges of technical and social interactions requires the establishment of clear procedures for early detection and counteraction against hybrid threats, including disinformation and cyberattacks. An integrated strategy necessitates multidimensional solutions, combining effective governance and social policies with technical measures, striking a balance between technological advancement and the stability of national communication and cybersecurity systems.

Ensuring security in Society 5.0 requires robust institutional mechanisms. Moreover, fostering multi-stakeholder cooperation, involving the public sector, private sector, and civil society, is crucial. Expanding the scope and developing the expertise of human resources is a strong aspect of combating these threats. This is particularly significant in terms of effective human resource management in a broader context [18]. Such a focus on human resource management would likely attract more potential employees to these organizations and be crucial for balanced career and personal development [19].

The fundamental transformations associated with manipulative informational influence necessitate unified efforts to protect interconnected technological and social systems. From a technological and cybersecurity perspective, these challenges appear more structured; however, in the context of social systems and communities, vulnerabilities in protection seem more pronounced. Information, humans, and technology form the cornerstone in the pursuit of communication security, understood as a complex system of interconnected elements aimed at reducing societal vulnerabilities [20].

The "human-centric" paradigm is oriented toward Society 5.0, a society that integrates digital, physical, and social spheres [21]. The sustainable development of Society 5.0 requires a holistic approach, combining innovative technological solutions, a strong strategic and regulatory framework, and robust cross-sector partnerships. In the sustainability journey that started with the 2030 SDGs, sustainability impacts have begun to emerge in every sector and in most social and economic areas of human life. [22].

Only through a balanced integration of the constituent constructs of information-communication interaction can we effectively protect the information space, minimize risks from negative informational influence, and maintain the stability of social and cyber systems.

REFERENCES

[1] E. Rosenbach and K. Mansted, The Geopolitics of Information, Defending Digital Democracy Project, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, 2019. [Online]. Available: https://www.belfercenter.org/publication/geopolitics-information. [Accessed: Feb. 14, 2025].

[2] R. Marinov, S. Stoykov, and P. Marinov, "Urbanized Territories Non-Existing Part of Crisis Response Operations," 2019 International Conference on Creative Business for Smart and Sustainable Growth (CREBUS), Sandanski, Bulgaria, 2019, pp. 1-4, doi: 10.1109/CREBUS.2019.

[3] C. Wardle and H. Derakhshan, Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking, Council of Europe, 2017. [Online]. Available: https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c. [Accessed: Feb. 14, 2025].

[4] A. Krishna and T. L. Thompson, "Misinformation about Health: A Review of Health Communication and Misinformation Scholarship,"2021, American Behavioral Scientist, vol. 65, no. 2, pp. 316–332, 2021. doi: 10.1177/0002764219878223.

[5] A. Gelfert, "Fake News: A Definition," Informal Logic, vol. 38, no. 1, pp. 84–117, 2018. [Online]. Available: https://philpapers.org/rec/GELFNA. [Accessed: Feb. 1, 2025]. p. 15

[6] E. C. Tandoc Jr., Z. W. Lim, and R. Ling, "Defining 'Fake News': A Typology of Scholarly Definitions," Digital Journalism, vol. 6, pp. 137–153, 2017. doi: 10.1080/21670811.2017.1360143. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/21670811.2017.1360143. [Accessed: Feb. 9, 2025].

[7] P. Dimov and E. Ivanov, Fake News: Recognizing Fake News and Disinformation in the Modern Hybrid Security Environment, Sofia, 2020, p. 21. [Online]. Available: https://rndc.bg/wp-content/uploads/2020/05/FakeNews-21-05-2020-pechat.pdf. [Accessed: Feb. 1, 2025].

[8] European Parliament, "Tackling Disinformation," 2017. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/ATAG/2017/599386/EPRS_ATA(2017)599386_BG.pdf. [Accessed: Feb. 1, 2025].

[9] The European External Action Service, "Tackling Disinformation and Foreign Information Manipulation," 2024. [Online]. Available: https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en. [Accessed: Feb. 14, 2025].

[10] European Commission, Tackling Online Disinformation: A European Approach, 2018. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236. [Accessed: Aug. 28, 2024].

[11] V. Vasilev, D. Stefanova, and C. Popescu, "Human Capital Management and Digitalization - From Good Practices and Traditions to Sustainable Development," in Digitalization, Sustainable Development, and Industry 5.0: An Organizational Model for Twin Transitions, 2023, pp. 41–65. doi: 10.1108/978-1-83753-190-520231004.

[12] N. Dolchinkov, "Construction of a System for Monitoring the Pollution of Water Bodies with Waste," ETR, vol. 1, pp. 136–141, Jun. 2024, doi: 10.17770/etr2024vol1.7989.

[13] Law on Strategic Planning of the Republic of Bulgaria. [Online]. Available: https://www.strategy.bg/FileHandler.ashx?fileId=16428. [Accessed: Aug. 28, 2024].

[14] The Updated National Security Strategy of the Republic of Bulgaria, 2018, pp. 7-8 [Online]. Available: https://www.me.government.bg/files/useruploads/files/akt.strategiq2020.pdf. [Accessed: Feb. 11, 2025].

[15] Updated National Cybersecurity Strategy "Cyber Resilient Bulgaria 2023." pp. 10, 13, 49, and 58 [Online]. Available: https://egov.government.bg/wps/portal/ministry-meu/strategies-policies/cybersecurity/cyber-legislation. [Accessed: Feb. 11, 2025].

[16] M. Modeva, The Non-Verbal Communication of the Political Leader, Sofia, 2022.

[17] K. Kazakov, "Fake News as a Tool for Manipulating Public Opinion," in Knowledge Society and 21st Century Humanism: The 19th International Scientific Conference, Sofia, Bulgaria,

Nov. 1, 2021, pp. 438–444. Sofia: Za Bukvite – O Pismeneh, 2021. ISSN 2683-0094.

[18] V. Vasilev, D. Stefanova, and M. Icheva, "Green Human Resource Management as a Component of Sustainable Organizational Development in Environmental and Natural Economics," ETR, vol. 1, pp. 402–407, Jun. 2024, doi: 10.17770/etr2024vol1.7966.

[19] R. Marinov, "Contemporary Challenges to the Protection of the Country's Sovereignty," ETR, vol. 4, pp. 168–172, Jun. 2024, doi: 10.17770/etr2024vol4.8187.

[20] D. Stefanova, "Security in Public Communications - Myth or Reality?," in Proceedings of the XXV Summer School in Public Relations, 2023, pp. 160–171. Sofia: NBU, 2023. ISBN 978-619-233-278-5.

[21] D. P. Stefanova, V. P. Vasilev, and I. P. Efremovski, "Re-Innovative Organizational Design: Sustainable Branding and Effective Communication - Applied Models in a World With New Borders/Without Borders," in Handbook of Research on Achieving Sustainable Development Goals With Sustainable Marketing, pp. 112–127, 2023. doi: 10.4018/978-1-6684-8681-8.ch006. Available: https://www.igi-global.com/gateway/chapter/325452#pnlRecommendationForm. [Accessed: Feb. 11, 2025].

[22] S. Yıldırım and V. Vasilev, "The Future of Green Collar Workers: Green Transition in Employment," in Green Transition Impacts on the Economy, Society, and Environment, S. Yıldırım, D. Yıldırım, I. Demirtaş, and V. Kandpal, Eds. IGI Global Scientific Publishing, 2024, pp. 1-16. doi: 10.4018/979-8-3693-3985-5.ch001.

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 297-301

Prerequisites for the Establishment of a Quantum Steganography Communication

Veselka Stoyanova
Artillery, AD and CIS faculty
National Military University Vasil Levski
Shumen, Bulgaria
veselka_tr@abv.bg

***Abstract*— Several approaches and techniques exist to make communication via the internet secure, one of these approaches is steganography. Computer steganography can be defined as a method of hiding data in cover media so that others are not aware of its existence. Quantum computers, built on the principles of quantum physics, have introduced new possibilities for researchers in security and computer science. This paper explores the fundamentals of quantum computing, its achievements, and the challenges and future prospects it presents in the field of cryptography and steganography. Quantum computers give us a new approach to different kinds of complicated problems in security fields by creating multi-state computing spaces. The article deals with the steganography system which hides text inside images and after that realize quantum communication. The secret message is hidden in the cover image using Least Significant Bit (LSB) algorithm. The paper proposes an information transmission scheme with a quantum channel enabled. Quantum key distribution (QKD) is a secure communication method that implements a cryptographic protocol involving components of quantum mechanics**

Keywords*— *Quantum Key Distribution, Quantum Steganography, Qubits, Security.

I. Introduction

Nowadays in the world of information technologies, unprotected and obviously data transmission is tantamount to suicide. The use of steganography, in close connection with cryptography and securing with static passwords in the authentication process protects against the high risk of information security.

Quantum computers give us a new approach to different kinds of complicated problems in security fields by creating multi-state computing spaces.

In classical computing, the basic unit of information is the bit, which can be either a 0 or a 1. In contrast, quantum computing uses qubits, or quantum bits, which can exist in a state of 0, 1, or both simultaneously, thanks to a property called superposition. This allows quantum computers to perform many calculations at once, making them potentially much more powerful for certain tasks compared to classical computers. [1] told us that we can imagine a spinning coin, representing both heads and tails until it lands – that's the essence of superposition, a quantum phenomenon defying classical logic yet unlocking immense computational potential.

Computer steganography conceals the existence of secret information in the cover carrier [2], [3], [4] and [5].

The study aimed to analyze the possibility of secure use of steganography in the implementation of quantum communication.

Quantum steganography leverages the principles of quantum mechanics, such as superposition and entanglement, to hide information within quantum states [6]. This makes it even more secure compared to classical steganography, as any attempt to intercept the hidden information would disturb the quantum state and reveal the presence of eavesdropping [7].

The quantum steganography can indeed be used in quantum communication [8]. The firewall works based on the consistent application of rules that are divided into two parts [9], [10].

In figure 1 we can see the potential of quantum steganography, which could to address various security and privacy challenges. It is extremely interesting that these areas could expand and almost no area of people's public life would be untouched. A wide field for research opens up. Quantum steganography will strengthen the resilience of quantum cryptography, due to the fact of absolute imperceptibility.

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8485
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.



Fig. 1. Applications of quantum steganography

II. MATERIALS AND METHODS

A. *Basic characteristics of Quantum steganography algorithms evaluation.*

Least Significant Bit (LSB) replacement is the process of adjusting the most significant bits of the pixels of the cover image [11]. More details about how work LSB could be found in [12-15]. Steganography provides a way to transfer this information via ordinary files, thus reducing the risk of disclosure [16].

Least Significant Bit Qubits (LSBq) is presented in [17], [18] and [19]. In this case, embeds the secret message's qubits to the carrier image's least significant qubits, researchers increased *LSB's* security by embedding it by a modulo value rather than in order. However, there have the limitations: using primarily *LSBq* makes it easy for intruders to detect and extract the steganographic image and can result in low imperceptibility.

When comparing two images four major statistical properties which describe the degree of similarity between the images are calculated: *MSE* (Mean Squared Error), *PSNR* (Peak Signal-to-Noise Ratio) and images entropy.

The characteristics studied are represented by formulas (1) and (2), the PSNR is based on values obtained for the MSE:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j)-K(i,j)]^2, \qquad (1)$$

where m and n are the width and height of the image; I (i, j) and K (i, j) are relevant pixels with coordinates (i, j) in the original stego-image.

$$PSNR = 10.log_{10}(\frac{max^2}{MSE}) = 10.log_{10}(\frac{max}{\sqrt{MSE}}), \qquad (2)$$

where max = 255 for 8 bit images.

Entropy is a statistical measure of randomness that can be used to characterize the texture of the input image. The entropy of an image can be calculated by calculating at each pixel position *(i, j)* the entropy of the pixel-values within a 2-dim region centered at *(i, j)*.

$$entropy = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} p(i,j)log\log_b p(i,j) \qquad (3),$$

where n and b are again the number of gray levels and the base of the logarithm function, respectively, and *p(i, j)* stands for the probability of two pixels separated by the specified offset having intensities *i* and j.

Quantum Mean Squared Error (QMSE) is typically used to quantify the difference between a target quantum state and an estimated quantum state. The calculation depends on the context, but here are the common approaches

QMSE-One approach uses fidelity

$$F(\rho,\sigma) = Tr\left(\sqrt{\sqrt{\sigma}\sqrt{\rho\sigma}}\right)^2 \qquad (3)$$

to compare two quantum states ρ and σ, where ρ is the target state and σ is the estimated state. A common definition of QMSE in this context is (4):

$$QMSE=1-F(\rho,\sigma) \qquad (4)$$

where $F(\rho,\sigma)$ is the fidelity between the density matrices.

The formula for QPSNR (5) is derived from the traditional PSNR formula and is expressed as:

$$QPSNR = 10.log_{10}(\frac{max^2}{MSE}), \qquad (5)$$

where MAX is the maximum possible pixel value (for example, 255 for an 8-bit image).

In [20] proposed a new model based on *log-polar* coordinates (quantum log-polar image, *QUALPI*). A log polar image with a resolution *of* 2^mX2^n and a gray level of *q2* can be represented by the following equations.

$$|I\rangle = \frac{1}{\sqrt{2^{m+n}}}\sum_{\rho=0}^{2^m-1}\sum_{\theta=0}^{2^n-1}(|g(\rho,\theta)\rangle \otimes |\rho\rangle \otimes |\theta\rangle \quad (\text{[20]})$$

$$g(\rho,\theta) = C_0C_1\cdots C_{q-2}C_{q-1}, g(\rho,\theta) \in [0, 2^q-1]$$

Here, *p* represents information of the image in the radial direction, *Θ* represents information of the image in the axial direction, and *(p, Θ)* represents the position information of the image pixels. *g (p, Θ)* represents the gray value of the pixel. In addition, the preparation process of quantum images is given in detail in [20].

III. RESULTS AND DISCUSSION

A. *Quantum steganography protocol.*

The quantum analogue of the *classical binary symmetric channel* (BSC) is the *depolarizing channel* (DC) which is one of the most widely used quantum channel models:

$$\rho \rightarrow N\rho = (1-p)\rho + \frac{p}{3} X\rho X + \frac{p}{3} Y\rho Y + \frac{p}{3} Z\rho Z \quad (6)$$

That is, each qubit has an equal probability of undergoing an X, Y or Z error. Applying this channel repeatedly to a qubit will map it eventually to the maximally mixed *state* $\frac{I}{2}$.

It is possible to rewrite this channel in a different but equivalent form:

$$N = \left(1 - \frac{4p}{3}\right) I\rho + \left(\frac{4p}{3}\right) T\rho \quad (7)$$

where $I\rho = \rho$ and

$$T\rho = \left(\frac{1}{4}\right)(\rho + X\rho X + Y\rho Y + Z\rho Z) \quad (8)$$

The operation $T\rho$ is twirling: it takes a qubit in any state ρ to the maximally mixed state $\frac{I}{2}$. If was rewritten the channel in this way, instead of applying *X, Y, or Z* errors with probability $\frac{p}{3}$, we can think of removing the qubit with probability $\frac{4p}{3}$, and replacing it with a maximally mixed state.

The figure 2 makes the steganographic protocol more transparent. It will possible at first assume the actual physical channel between Alice and Bob is noiseless. All the noise that Eve sees is due to deliberate errors that Alice applies to her codewords.

Step 3 share with us how Alice chooses a random subset of *M* qubits out of the *N*, and swaps her *M* stego qubits for those qubits of the codeword. She also replaces a random number *m* of qubits outside this subset with maximally mixed qubits, so that the total *Q=M+m* matches the binomial distribution (6) to high accuracy.

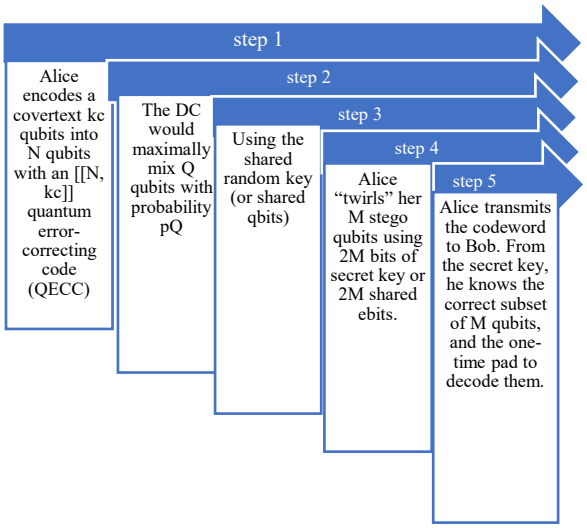


Fig. 2 Visualization quantum steganography protocol.

Generate two entangled qubits: *QubitA* and *QubitB*, such that their states are correlated. *QubitA* was prepared in a superposition state that will represent the hidden information. The specific state preparation depends on the encoding method chosen [1].

B. Simplified conceptual quantum algorithm.

The figure 3 provides and included a short description of scheme methodology of simplified conceptual quantum algorithm.

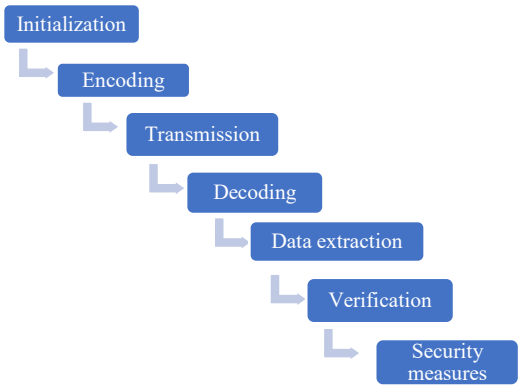


Fig. 3. Flowchart of simplified conceptual quantum algorithm for communication.

It's (9) to calculate the maximum number of secret information's bits transmitted per time.

$$[X]_{max} = log2\frac{360^0}{\theta} \quad (9)$$

where, is θ smaller than the minimum rotation angle at which the image is expanded, and $[X]_{max}$ denotes the maximum number of secret information's bits by calculation.

Finally, quantum communication in free space involves many basic infrastructure elements that are extremely important for any quantum communication link. They are also critically important due to the direct impact on the reliability, security and efficiency of the quantum communication node.

IV. Other Recommendations

A. The future of secure quantum communication

One of the main aims of the realized research of the steganography system is its practical applicability and evaluation in terms of the invisibility and size of the hidden data in the cover images.

Steganography algorithm for embedding information in images uses the *LSB* in each colour channel pixels and after that used quantum channel to send a key. How this works presented on figure 4, a stego image can use an opened communicate channel.

Thus, it is checked and ensured what operation will be implemented and the confidential information is preserved. This is the basic communication scheme with the steganographic environment included.

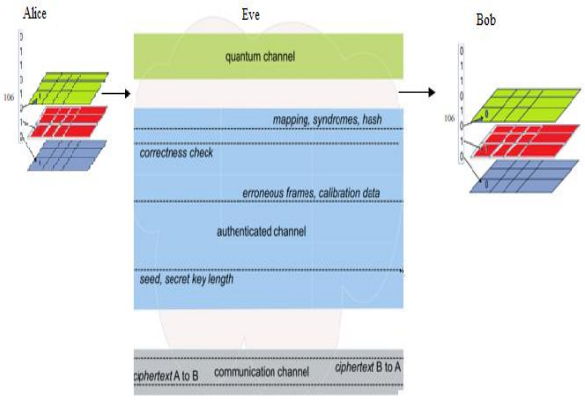


Fig.4. LSB Replacement embedding in colour image using quantum channel.

QKD is a part of quantum cryptography [21]. It is a secure communication method for exchanging encryption keys only known between shared parties. *QKD* network architecture can to be seen in figure 5:

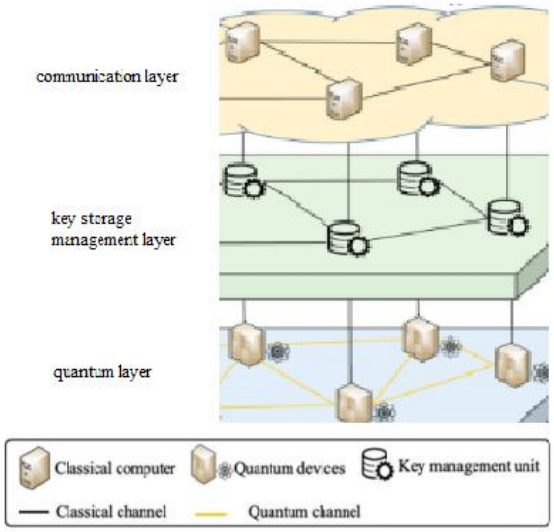


Fig.5. Communication scheme on layers on the QKD network.

A wide area *QKD* network is composed by a set of quantum, point to point, nodes linked by quantum channels. These links could also include information theoretic security (ITS) switched networks, like the access network depicted at the lower rigth corner. The set of quantum nodes and links form the quantum level. Many of the quantum nodes will act as classical repeaters by retransmitting the keys distilled from the signals of one of the quantum links using another quantum link connected to the same node [21]. In general scheme of the communication could establish three layers – communication layer (Key users, for example encryptors), key storage management layer (Protection of the encryption keys via using *QKD* keys for every hop) and quantum layer (Key Generation –symmetrically independent).

B. Quantum Key Distribution.

In general, *QKD* is combined with conventional encryption systems, such as AES, where the generated *QKD* key is used by Alice and Bob to generate a temporary session key with AES, to encrypt their messages over Ethernet until it expires, and *QKD* protocols require the ability to create, manipulate, transmit and detect signals at the quantum level.

When the cover protocol consists of communicating classically over a quantum channel, we show that, in addition to the cover classical message, entangled qubits can be generated [22]. Currently, the number of qubits that can be controlled and manipulated in a laboratory environment is still very small, limiting the potential of quantum computing. Another fundamental problem of a quantum computer is how to send and receive information from it. Some critics consider this problem insolvable. However, this appears to be less of a problem in optical quantum computers where qubits are defined in terms of photons [1]. In [23] is presented the hierarchical decision model of cybersecurity risk assessment.

V. Conclusions

In conclusion, this paper encompasses a discussion on the field of quantum steganography, which is a process of hiding information in existing content. Mostly images are used to hide the content. Unlike classical steganography, which hides information in plain sight, quantum steganography leverages quantum entanglement and superposition to encode data in quantum states, making it exceptionally resistant to unauthorized interception or decryption.

In the local way had have lack of understanding regarding the necessity of *QKD* implementation, the equipment has high prices and lack of standards, but QKD is likely the most advanced quantum technology currently accessible in use. With the increase in computing power, cyber security is getting complicated.

The importance of the use Quantum Steganography as a means to hide sensitive information through public channels by governments, companies and individuals are important. This is because countries exchange confidential information in their daily activities. Least significant qubit: uses the carrier image's least significant qubits to embed the needed secret qubits.

Acknowledgement

The author would like to thanks that paper was supported by the NSP DS program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022

References

[1] M. Imanparast, "The prospect of cryptography and computing with quantum computers", 8th International Conference on Combinatorics, Cryptography, Computer Science and Computation, pp.379-384, 2023.

[2] N. Subramanian, S. Al-maadeed, A. Bouridane, "Image Steganography: A Review of the Recent Advances", IEEE Access, vol. 9, 2021, pp.23409-23423, doi:10.1109/ACCESS.2021.3053998.

[3] P. Mandal, I. Mukherjee, G. Paul, B. Chatterji, "Digital image steganography A literature survey", Information Sciences,

Elsevier Inc, volume 609, 2021, pp. 1451–1488, ISSN: 0020-0255, [Online]. Available: doi.org/10.1016/j.ins.2022.07.120

[4] D. Artz, "Digital steganography: hiding data within data", in IEEE Internet Computing, vol. 5, no. 3, pp. 75-80, 2001, doi: 10.1109/4236.935180

[5] V. Stoyanova, "Research of the characteristics of a steganography algorithm in images when using different alphabet" Environment. Technologies. Resources. Proceedings of the International Scientific and Practical Conference. Vol. 4. 2024, https://doi.org/10.17770/etr2024vol4.8236.

[6] A. Agrawal, R. Soni, and A. Tomar, "Perspective Chapter: Quantum Steganography – Encoding Secrets in the Quantum Domain" in Steganography - The Art of Hiding Information. IntechOpen, Apr. 19, 2024, doi: 10.5772/intechopen.1004597.

[7] B. A. Shaw, T. A. Brun, "Quantum Steganography", arXiv:1006.1934, 10 Jun 2010, https://doi.org/10.48550/arXiv.1006.1934

[8] N. Min-Allah, N. Nagy, M. Aljabri, M. Alkharraa, M. Alqahtani, D. Alghamdi, R. Sabri and R. Alshaikh, "Quantum Image Steganography Schemes for Data Hiding: A Survey", Applied Sciences, 12(20), 2022, 10294. https://doi.org/10.3390/app122010294

[9] Ts.Tsankov, L.Staneva, I.Vardeva and D.Iliev, "Generalized net model of a communication network using the Port Knocking method", Scientific Conference with international participation MATTEH 2022, Conference proceeding, Vol. 2, Shumen, 2022, ISSN 1314-3921, pp. 29-34

[10] Ts.Tsankov, T.Trifonov and L.Staneva, "A survey of phase manipulated signals with high structural complexity and small loses after processing with mismatched filters", Konstantin Preslavski University Of Shumen, Jornal Scientific and applid reserch, 2013, https://jsar.ftn.shu.bg › jsar › article › download, [Accessed Yan 24, 2025].

[11] V.Stoyanova, "Steganography System Using LSB Methods", Proceedings of the ENTRENOVA. ENTerprise REsearch InNOVAtion Conference, Split. Croatia, IRENET – Society for Advancing Innovation and Research in Economy, Zagreb. 6–8 .09.2018. Vol. 4. P. 381–387

[12] M.Al-Shatnawi, "A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, vol. 6, no. 79, pp. 3907 – 3915, 2012.

[13] C. K.Chan and L. M.Cheng, "Hiding data in images by simple LSB substitution", Pattern Recognition, vol. 37, pp. 469-474, 2004.

[14] C. C. Chang, J. Y. Hsiao and C. S. Chan, "Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy", Pattern Recognition, vol. 36, pp. 1583-1595, 2003.

[15] C. H.Yang and S.-J.Wang, "Transforming LSB Substitution for Image-based Steganography in Matching Algorithms", Journal of Information Science and Engineering, vol. 26, pp. 1199-1212, 2010. [Online]. Available: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=fe144037adc9e934a44cb1f31aaee4ed5cb4cd2e, [Accessed Yan 24, 2025].

[16] G. A. Kozarev and St. H. Parvanov, "Research opportunities for using steganographic methods in the field of defense", Proceedings of International Scientific Conference-Defense Technologies‖ DefTech 2024, Shumen, pp.637-642, ISSN 2367-7902.

[17] R.G.Zhou, J.Luo, X.Liu, C.Zhu, L.Wei and X.Zhang, "A novel quantum image steganography scheme based on LSB", International Journal of Theoretical Physics, June 2018, 57, 1848–1863, DOI: 10.1007/s10773-018-3710-x.

[18] A.G.Tudorache, V.Manta and S.Caraiman, "Quantum Steganography Using Two Hidden Thresholds", Adv. Electr. Comput. Eng. 2021, 21, 79–88.

[19] E. Şahin, I.Yilmaz "QRMW:Quantum representation of multi wavelength images", Turk. J. Electr. Eng. Comput. Sci., 7, 2018, pp.68–779.

[20] Y. Zhang, K. Lu, Y. Gao, and K. Xu, "A novel quantum representation for log-polar images," Quantum Inf. Process., vol. 12, no. 9, pp. 3103_3126, Sep. 2013.

[21] V. Martin, M.J.Martinez and M.Peev, "Introduction to Quantum Key Distribution", 2016, http://www.gcc.fi.upm.es/publications/qkd_intro.pdf

[22] M. Tahmasbi and M. R. Bloch, "Steganography protocols for quantum channels", Journal of Mathematical Physics, vol.61, issue 8, August 2020;082201. https://doi.org/10.1063/5.0004731

[23] V. Petrova, "The Hierarchical Decision Model of cybersecurity risk assessment", 12th National Conference with International Participation (Electronica), vol. 1, 2021, pp. 1-4, doi:10.1109/ELECTRONICA52725.2021.9513722. 978-1-66544061-5.

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025 Volume V, 303-309

Defense Concept Through the Legislature - Protecting Values for the Sustainability of Society

Dace Šulmane
Faculty of Law
University Turība
Riga, Latvia
dace.sulmane@gmail.com

***Abstract*— The pivotal function of independent institutions in the adjudication of legally binding decisions, in accordance with the rule of law and the fundamental principles of the Latvian legal system, is evident. These institutions serve to clarify and adjust the applicability of general concepts to specific cases that are the subject of dispute. The unique geopolitical situation of Latvia is a perpetual reminder of the ambiguity with which its state institutions are regarded by the public and other state-level actors. A fundamental and diametrically opposed clash of opinions within the framework of the state itself (between various stakeholders, members of society, political players, institutions) and in the mass media environment, inciting long-term disagreements and turbulence, can literally be created by a few words or one sentence, one illustration, from the context of which the author's opinion on global issues of Latvian history and political position can be interpreted more broadly. The concept of militant democracy involves the potential questioning and challenging of the very guarantees of defending freedoms and human rights. The article provides a critical overview of the latest amendments to legislation and court practice, thereby establishing a unique insight into the ability and methods of all three powers of the state in strengthening and defending state values in times of turbulence.**

Keywords*— *boundaries of freedom, fundamental values, ideologies, militant democracy

I. Introduction

While "law" is undoubtedly associated with a high degree of abstraction, theories about the force of legal rules and methodologically correct application, "politics" is a process of struggle between different interests and ideologies, materialised in parliament and government through decisions that are binding on society. In Latvia, the relevance of the concept of 'ideology' in the light of geopolitical developments is indisputable, and at the same time it has been recognised that the study of ideology in the social sciences is fragmented rather than productively integrated. Looking at the contemporary legal-political realities of post-Soviet countries, two simultaneously actively used options for the application of ideological positions can be identified: direct (legislative) and indirect (through the legal enforcer - the judiciary/institution). The legislator can adopt explicitly ideologically filled normative acts in order to emphasise *expressis verbis* the importance of an idea, a new development trend, an ideological consideration for the future development of the state. At the same time, the dynamic division of opinion in democratic societies creates a constant conflict between "permitted" and "unauthorised" opinion, between the delicate boundaries of freedom of expression and hate speech, and between clear legal "red lines" between healthy political debate in a free democratic society and conduct that is deemed anti-government, punishable, unacceptable. Significant internal changes have also been observed, particularly in the Baltic states and Poland. Firstly, the local Russian-speaking population in the Baltic states has become increasingly polarised and mobilised, predominantly in support of Putin's imperialistic objectives and in opposition to providing assistance to Ukraine. [1]

It could be posited that the EU executive's augmented role in EU defence matters reflects a comprehensive consensus within the Union and among its member states on a political and strategic posture to be adopted in this policy domain. Nevertheless, while consensus has been achieved regarding the Commission's increased involvement in EU defence policy, this shift relates more to the EU executive's economic responsibilities, especially its control over Union funds, rather than indicating a political-strategic direction for EU defence. [2] Member States establish national defence and security strategies based on political and geographical factors. As a result, legislation and sanctions for prima facie similar cases can vary widely, and it is up to decision-makers in each country to analyse risk factors and regulate society accordingly. For example, in 2024, the Latvian legislator strengthened

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8511
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

responsibility for crimes against national security in the Criminal Code. Assistance to a foreign country in an act directed against Latvia can be punished with imprisonment for up to ten years instead of the previous five years.

As recognised in the publications of Latvian legal scholars, it is primarily the legislator who has to take care of the concretisation and implementation of the principle of militant democracy (or self-defensive/self-protective democracy) by adopting laws to introduce appropriate instruments for the protection of a democratic state governed by the rule of law. [3] It should not be assumed, therefore, that the judiciary or the executive should be the first bastion for the defence of the state and the safeguarding of democracy. There needs to be a clearly defined body of law that conveys a comprehensive understanding that the legislature takes potential threats seriously and is able to define criteria that distinguish with legal precision between perceived and real threats to security and public order, and to regulate the prevention of risks in a pre-emptive manner.

II. Materials and methods

The development of the article is founded on the selection and implementation of various scientific research methodologies. The following fundamental research methods have been employed: the method of analysis and synthesis, the comparative method, the historical method, and the descriptive method. The analytical method allows to identify the main issues of concern in the content of the sources, as well as to focus on their novelty, relevance or shortcomings. The comparative method has been used mainly to find commonalities and signs of development in the findings of Latvian and foreign legal scholars, as well as to provide insight into Latvian and European case law. The descriptive method allows the article to be understood in a sequential way and the chain of reasoning behind the conclusions to be traced.

The selection of sources was made with the objective of analysing and establishing how amendments to the normative framework interact with the practice of law enforcement (by state institutions and courts), as well as with the conceptions of state values developed by legal science and public policy makers.

In this article, combining insights from legal theory and political science, the author illustrates the complex socio-psychological factors that, in the historical mentality of post-Soviet society, make the judiciary balance between legal norms created by the legislator through the result of teleological interpretation of legal norms towards an interpretation that must be in line with the national, ideological values defined in the preamble of the Constitution.

The article is original research based on primary sources in order to conduct the most authentic qualitative research on the official assessment and justification of Latvian public officials to balance security considerations in preserving the unity of society and statehood.

III. Results and discussion

A. Securing the State Values Through Legislation and Protective Procedural Measures

The first Latvian Saeimas after the restoration of Latvia's independence adopted a number of laws to prevent persons who had actively expressed their rejection of Latvia's existence as a democratic state from participating in the institutions that ensure Latvia's state functions (e.g. exclusion from the Supreme Council of deputies who had acted against Latvia's independence, ban on organisations of political organs of the Soviet authorities that opposed Latvia's independence, ban on passive voting rights - prohibiting certain persons from participating in the political process). The restrictions were mainly directed against persons who, very recently before the adoption of the relevant restrictions, actively tried to delay the establishment of a democratic Latvian state and its return to the family of democratic states, and their purpose was to protect Latvia's national security and democratic state apparatus. For example, the Citizenship Law established detailed restrictions on the acquisition of Latvian citizenship through naturalization for those persons who, after the regaining of Latvia's independence on May 4, 1990, expressed communist or other totalitarian ideas or incited national or racial hatred or discord, worked in an anti-state or criminal organization. [4]

The prohibition of non-democrats from forming the politics of an independent state has proven to be a partially effective and resource-intensive measure. For instance, the American law and politics professor Cary Coglianese, in his article entitled "Law as a Scapegoat", rightly observed the frequently observed phenomenon of populist leaders attributing blame to the regulatory system and specific legal regulations, which they claim are responsible for economic and social problems and upheavals. Consequently, populists (a phenomenon also observable in some European countries) have been successful in undermining public trust in the legislature and challenging the notion of democratic legitimation in relation to the state's overarching objectives. [5]

The fundamental values of the Latvian state cannot be violated or changed, and therefore the Constitutional Court has clearly recognised that amendments to the Satversme that would violate the fundamental norm of Latvia would be unconstitutional. Thus, the Latvian legal system is structured in such a way that even if populist or radical parties were to gain a majority in Parliament, amendments that would revise or abolish the fundamental norm enshrined in Latvian jurisprudence that "Latvia is a democratic state governed by the rule of law" would not be valid. When it comes to defending the founding idea of the Latvian political regime and the rule of law, one cannot rely solely on the political will of the majority of the population. States usually require a much larger majority for important decisions, such as the quorum requirements for the Saeima or for the body of Latvian citizens to decide on the basic foundations of the state (Articles 76-79 of the Constitution). As historian G. Zemītis has pointed out, "opponents of the republican and democratic order can also

come to power as a result of elections", and democracy is particularly threatened when the government has to take unpopular decisions. [6] Each country develops its own legal instruments to deter potential beneficiaries or to warn them at a very early stage of the negative consequences of any action against the democratic rule of law.

The most notable push toward militant democracy was the adoption of the Preamble to the Constitution in 2014. After the unequivocal results of the referendum, which strongly rejected a proposal on the second national language, the Latvian legislature and the executive branch mobilized to highlight the need for the process of "ideological education". Already two years later, as a known response to the referendum, the Preamble to the Constitution entered into force. It was developed for the purposes of stability and value orientation of the country after the referendum on the second national language (Russian).[7]

A novelty in adapting the regulatory framework to the new risk and threat situation, in order to ensure the functioning of the state apparatus and the value orientation of the next generation of Latvians, have been the amendments to the laws (2017) that provide for the requirement of loyalty to a democratic legal state when a person exercises his or her right to participate in the activities of the state and local governments and to perform public service (last school teachers), as provided for in Article 100 (freedom of expression) and Article 106 (right to freely choose their employment and workplace) of the Constitution.

The Constitutional Court and the European Court of Human Rights have recognised the principle of militant democracy (democracy capable of defending itself) as a general legal principle on which to base arguments concerning threats to the existence and security of the state. In examining the conformity of legislative acts, the Court noted that "the Baltic States, in the transition from totalitarianism to democracy, had to deal with a double task, i.e. the restoration of both the democratic regime and national sovereignty. In addition, Latvia was particularly affected by the colonisation policy of the USSR".[8] In Latvia, the country that suffered the most from Russification of all the Baltic states (in 1988 only 52% of schools taught in Latvian, in 1980 the proportion of Latvians in the country was only 52%, the real national policy was never fully visible, but masked, there was pressure for "Russification"), demagogic tools are used to create an argument that is very difficult to distinguish from the abusive use of democracy to eliminate the rule of law (the principle of the rule of law).

The role of both the constitutional courts and the general courts is to draw these "red lines" independently and methodologically correctly. Ideologically neutral legal ideals such as general principles of law, the democratic state, guarantees of the rule of law, fundamental rights, etc., allow problems to be solved within the profession without getting involved in the vicissitudes of political science. Lawyers and the judiciary are not disconnected from society, and it is therefore impossible for the judiciary to avoid, at the stage of applying the law, resolving legal disputes that have arisen or are directly caused by the different positions of the parties to a dispute on ideological issues.

The practice of the Constitutional Court and the European Court of Human Rights has been established with regard to banning opponents of Latvia's independence from participating in political processes. In this context, there is no more effective concept to justify the actions of the state than the development of the principle of militant democracy. It is worth quoting the Constitutional Court's statement that "a democratic state system must be protected from persons who are not ethically qualified to be representatives of a democratic state at the political or administrative level and who have proved by their actions that they were not loyal to the democratic state system, i.e. from persons who worked in the apparatus of direct oppression and direct repression implemented by the occupying power and from persons who, after the restoration of the independence of the Republic of Latvia, tried to restore the totalitarian state and opposed the legitimate state power".[9] There is a clearly recognised legal basis for prohibiting certain persons from performing public service, and this cannot be treated as an illegitimate violation of personal rights (for example, the prohibition of the right to employment). Due to the lustration applied by Latvia regarding the policy of citizenship and residence permits, several cases reached the ECtHR ("Sisojeva and others v. Latvia" and "Sļivenko v. Latvia").[10]

According to Latvian legal scholar J. Pleps, the protection of democracy implies significant restrictions on the fundamental rights of the individual and the political process in a democratic society. For this reason, it is necessary to take special care that the protection of democracy does not actually eliminate the democratic constitutional state. [11] With the slogan of the will of the people and the rule of the majority (which is essentially a fundamental feature of democracy), the defenders of democracy can use demagogic tools to create an argument that is very difficult to distinguish from the misuse of democracy to eliminate the rule of law (the principle of the rule of law).

Such a means of protection and public safety as the principle of prohibition of abuse of fundamental rights and instruments of a democratic legal state, provided for in Article 17 of the Convention, should be considered as an important consideration. "The very purpose of the Convention is to preserve and promote the ideals and values of a democratic society. In other words, democracy is the only political model envisaged by the Convention and therefore the only one compatible with it".

B. Protection of Democracy Through Restrictions - Case Studies

Threats to the state system very often manifest themselves through the actions of members of society - organised actions, the creation of various communities and structures - so that, despite the guarantees of freedom of

expression and freedom of association, state institutions must be constantly vigilant to protect the values of the state.

It is important to point out that Latvian jurisprudence recognises that in a well-functioning democratic state the principle of militant democracy should be directly applied only in very rare cases, otherwise it signals an insufficiently high level of alarm: radicalisation of social groups, open opposition to the ideals of the country's democratic state, contempt for the rule of law, disrespect for the functioning of state organs and disloyalty to the fundamental principles of the state.

The fact that security threats, illegal, anti-state actions always start with individual cases (a specific reported picket, the activity of a specific organisation, the actions of a specific person threatening the state apparatus, etc.), then the correct identification of such cases and the strict interpretation of regulatory acts in accordance with the values of the Constitution are of crucial importance. It is the individual cases that challenge the system and try to "break through" the protective wall created by the legislator in order to create cracks in the foundations of a legal state, to shake the confidence of state institutions in their actions (appeals to the highest instance, appeals to international institutions and lobbying for the opinions of foreign experts). These are the formats in which illiberal democracies can take shape, and as Poland's recent experience shows, dealing with personnel reforms in key public positions (judges appointed for life) in these phases of threat to the state regime is extremely problematic and a constant threat to the country's internal stability.

The evolving roles and functions of laws in modern Western democracies necessitate an examination of the regulatory framework that pertains to political parties themselves (a stage prior to the actual composition of parliament, which is often abstractly designated as a single entity in legal science – the legislature). Since the restoration of independence in the 1990s, the regulation of state law and also court practice have increasingly defined under which conditions freedom of speech and opinion is no longer freedom of speech and opinion, turning into a state threat and security risk. A notable paradox emerged in recent years, coinciding with the onset of the COVID-19 crisis. This crisis gave rise to a multifaceted landscape of opinions, characterised by a diversification of perspectives and a deepening of ideological divisions. Initially manifesting as a dichotomous concept, polarising between 'us' and 'opponents', this ideological landscape has evolved into a more nuanced terrain. It has transformed into a complex geometry of opinion groups, encompassing diverse positions such as 'us' and 'in certain issues us', 'opponents, but still us', and 'opponents that we do not tolerate, generally exclude from the discourse'.

In the Baltic countries, as in other post-socialist nations, nostalgia for communism remains a prevalent phenomenon. Despite condemnation from state officials, the Soviet past and its legacy are frequently portrayed positively in public discussions (among Russian speakers) and in everyday interpersonal communication (online Facebook groups, for example). [12]

Monitoring extremist/radical movements is the responsibility of the security authorities, but banning the establishment or activities of such organisations is only possible through decisions by state institutions; the legitimacy of decisions can be challenged in court. One example is a court ruling on the compatibility of commemorating the *pērkoņkrustieši* (the racist organisation "Pērkonkrusts" (eng-Thunder Crusaders) existed in Latvia in the 1930s and 1940s) with the principles of a democratic constitutional state, which was based on a ban on this type of ideology passed by the Latvian Parliament before the Second World War. In a sense, today's thundercrusaders openly identify themselves with a pre-war organisation defined by historians as one that sought to replace parliamentary democracy with a presidential state (dictatorship) through chauvinistic and even openly racist propaganda in order to implement extreme anti-Semitism. [13]

It is precisely in such cases that the court has referred in *expressis verbis* to the possibility of dishonest action directed against the fundamental principles of the rule of law: "It cannot be ruled out that a person or a group of persons will invoke the rights laid down in the Convention or its Protocols in order to obtain the "right" to act, which in practice means actions aimed at destroying the rights or freedoms laid down in the Convention; any such subversive action would put an end to democracy. No one should be allowed to invoke the provisions of the Convention in order to weaken or destroy the ideals and values of a democratic society".[14]

The former representative of the Communist Party of Latvia (T.Ždanoka) challenged in the Constitutional Court the lawmaker's ban on her applying for the Saeima elections, appealing to the fact that the contested norms are outdated and no longer comply with the Constitution. The Constitutional Court concluded that a person who cooperated with the totalitarian regime threatened the independence of the Latvian state and the principles of a democratic legal state with his actions, and even after two decades, democracy has not yet become generally accepted and self-evident in Latvian society, and there is no reason to believe that Latvian democracy has become sufficiently stable over time. [15]

It should be noted that ten years before that, the party "Par dzimto valodu!" (For the Mothertongue!) went all the way to the Supreme Court to claim for moral compensation against the then Minister Jānis Bordāns, because in 2012 a press release was published on the website of the Ministry of Justice with the title "Minister of Justice: the possibility of registration of political parties hostile to the state is a direct threat to democracy". The court recognized it as a person's opinion, therefore the consequences requested by the party (withdrawal of news) were not applied. [16]

Court practice in another case dealt with refusal to register an NGO called " Eirāzijas Savienība" (Eurasian Union) by the Register of Enterprises of the Republic of Latvia. One of the goals of the newly-established NGO was cooperation with Cossack associations of the world, as well as an appeal to the President of the Russian Federation with

a request to grant several Latvian cities the status of "Hero Cities". The NGO iniciators' arguments that "such a request is based on the 1965 decision of the Presidium of the Supreme Council of the USSR, which is still valid until the Saeima rejects it" is absurd and dangerous. Even more, expressing to the court that it is normal diplomatic practice to ask the President of another country to award a prize to a city of another country. [17] As pointed out by scholars, certain organisations focus their activities on falsifying the truth: the aim is to tell radical lies about history: to deny genocide or crimes against humanity, thus inciting hatred against a national or ethnic group. Organised groups, government officials and responsible employees of a company or organisation are often involved in planning and committing these crimes. [18]

At the end of 2024, the Supreme Court of Latvia passed a judgment on SIA "Masu Mediju grupa", which had received state funding for media support through a tender process, but which the Military Intelligence and Security Service had indicated in 2020 that the applicant's media had in the long term disseminated particularly aggressive, anti-Latvian propaganda messages. The court argued: "The use of state budget funds to support commercial media is permissible only in the common interests of the entire society, strengthening Latvia's information space and promoting high-quality and reliable content. The maintenance and propagation of Russian propaganda narratives, disinformation and fake news in the information space of Latvia with the support of state budget funds is not permissible and is against the interests of society." However, the *obiter dictum* court emphasized that one of the most important foundations of a democratic society is freedom of speech, but an ill-considered fight against disinformation threatens the right of every person to freedom of speech, as well as the independence of the media. [19]

Apparently, with the aim of confronting the understanding of the institutions of a democratic state about freedom of expression, the political party "Union of Russians of Latvia" had announced a march in May 2022 with the aim of expressing a protest against the actions of the ruling parties of Latvia, destroying Soviet monuments, prohibiting the use of traditions and the native language of minorities in education. By the decision of the executive director of the city of Riga, the planned march was prohibited. In the cassation claim, the applicant cynically manipulated the appeal to the guarantees of the European Convention for the Protection of Human Rights and Fundamental Freedoms (to ensure a peaceful march), the Constitution (violation of the presumption of innocence contained in Article 92 of the Constitution, violation of the prohibition of discrimination provided for in Article 91 of the Constitution). The reasoning of the Supreme Court clearly reflects the position of militant democracy: if there is a reason to conclude that the actions of the Russian Union of Latvia and its members echo the policy of the aggressor state and the announced march can create a platform for the expression of views supporting the aggressor state, then the state has a reason to act to prevent such a threat and protect the state itself and its democratic system. [20] On 9 May 2022, a significant congregation of predominantly Russian-speaking individuals convened at the Soviet Victory Monument in Riga to pay tribute to the liberation of the city from Nazi occupation and honour the Soviet troops who lost their lives during the Second World War. However, from the perspective of the Latvians, the Soviet Victory Monument represented the reoccupation of their nation by the Red Army. The congregation at the Soviet Victory Monument provoked a strong reaction from the Latvian populace, ultimately resulting in the resignation of the Minister of the Interior. [21]

The public's perception of current political events puts additional pressure on the mass media. In recent years, "firefighting" in the media environment has always been associated with provocations/apparent provocation or border violations in relation to the country's Eastern neighbour and war in Ukraine. In 2023, the National Council of Electronic Media sanctioned one of the media leaders "TVNET GRUPA" for a live interview with the political party "Stabilitāte!" containing the leader's statements about possible amendments to the "Immigration Law". By allowing the politician to speak uninterrupted, the program provided deliberately inaccurate information that the possible amendments to the Immigration Law provide for the deportation/ expulsion of citizens of the Russian Federation and Belarus (foreigners) from the country if they have not applied for the state language proficiency test and have not submitted an application for the status of a permanent resident of the European Union. The use of the term "deportation" by state institutions was recognized as unacceptable, taking into account Latvia's experience in the 20th century, suffering from mass deportations carried out by the totalitarian regime. [22] It is unequivocally concluded that the use of specific terms in Latvia has a completely different public safety background and danger than in other European countries.

On the second anniversary of the Ukrainian war, the highly heated media sensibility was unexpectedly created by the "Pig comic" of the Latvian artist G. Evelone published in the official media of Latvia, in which the Ukrainian nation was personified by a soldier-pig (as evidenced by the unmistakable inscription "Ukraine" on the pet's arm) with stylized, armor-like clothing and a weapon in his hands. As the media ombudsman admitted, this was a new precedent in the history of Latvian media communication, because the readers' reaction (which could be described as exaggerated dramatization), opposing the visualization of the tragedy of the Ukrainian people in the form of a pig, pointed to the extreme non-acceptance of this caricature tradition in Latvian society. The cartoon was immediately removed from the media environment. [23]

In 2024, a letter from Latvian Radio employees "The boundaries of freedom of speech are narrowing" was made public, stating that "there are situations when, predicting a wave of hatred, journalists do not want to create content on debatable topics or censor themselves in their coverage" and that "Russia's full-scale invasion of Ukraine has further

narrowed the boundaries of freedom of speech - only "patriotic" content is expected from the media, especially public ones, but the expression of an opinion contrary to the "mainstream" is evaluated as an anti-state act of the media".[24] Not in all cases the experts in various fields (art, media, education etc) agree with the interpretation of legal norms and decisions made by state institutions: this creates a conflict of diametrically opposite assessments on the basis of the restriction of fundamental rights. Although a democratic state does not have to wait until the relevant actions aimed at destabilizing the state apparatus have reached the level of danger, the state has the right and duty to prevent such a threat at an early stage, for understandable reasons in the society may be underestimated and criticized.

IV. CONCLUSIONS

In recent years, the Latvian legislature has significantly intensified amendments to regulatory acts that directly respond to provocations (to prevent them in the future), as well as proactively (to avoid or minimize public security threats, to discipline and protect democratic values). This is possible if the institutions representing the branches of state power are able to control and prevent possible excesses in the application of the principle of militant democracy.

The Latvian legal system is bound by a general legal principle that obliges it to protect and prevent the legal liquidation of the democratic legal state. This principle is derived directly from the Latvian legal system's basic norm.

E. Levits has stressed that liberal democracy should not be confused with value relativism and that there is no turning back from a democratic order: nor should it be possible to abolish human rights by non-democratic means, for example by abolishing term limits for senior public officials. It may sound paradoxical, but the statement that "democracy cannot be abolished democratically" not only clearly delineates the permissible limits of the abuse of democratic procedures in state life, but also points to the innate orientation of democracy towards the rule of law and human rights, which are at its very core. [25]

The concept of militant democracy is still in its development phase. In the context of political turbulence, legislators in democratic legal states often adopt a more cautious approach towards their citizens, perceiving risks and dangers in ambiguous situations. It is essential to ensure that self-defence does not cross the line and become a threat or an attack. A rule of law state is founded on the principles of rights and freedoms, the reliance on the good faith of society's representatives, honesty, loyalty and trust in fundamental rights. Consequently, the use of human rights should not be directed against democracy as such, and it is not always possible to legally define this difference precisely with the text of the law. This is precisely the reason why the judiciary plays a decisive role in the value-oriented interpretation of legal norms as an independent foundation stone independently of the ruling political rhetoric.

REFERENCES

[1] V. Veebel, “Strategic Challenges for Baltic States in Dangerous Times,” Journal on Baltic Security, vol. 9(2), pp.1-4, 2023.

[2] R. Kuokštytė, “EU Defence Policy: Between Functionalism, National Interests, And Transatlantic Realities,” Baltic Journal of Law & Politics, vol.16:2, pp. 23–46, 2023.

[3] J. Pleps, Pašaizsargājošās demokrātijas princips (The Principle of Militant Democracy). Jurista Vārds, vol. 51/52 (1317/1318), pp. 12-17, Dec. 2023.

[4] I. Švarca, Pārejas perioda taisnīguma mehānismi demokrātiskā Latvijā (Transition period justice mechanisms in democratic Latvia). Jurista Vārds, vol. 31 (1141), pp. 24-30, Aug. 2020.

[5] C. Coglianese, “Law as Scapegoat,” in The crisis and confidence in legislation. Eds. N. Lupo, N. Rangone, and M. De Benedetto. London: Bloomsbury Publishing, 2020, pp. 337-365.

[6] G.Zemītis, Drošības aspekti Latvijas vēsturē (Security aspects in the history of Latvia), Rīga: LU Akadēmiskais apgāds, 2023, p. 448.

[7] D. Šulmane, “Ideology, Nationalism and Law: Legal Tools for an Ideological Machinery in Latvia,” Wroclaw Review of Law, Administration & Economics, vol. 5(1), pp. 61-78, Jun.2015.

[8] Satversmes tiesas 2006. gada 15. jūnija spriedums lietā Nr. 2005-13-0106, para.17.

[9] Satversmes tiesas 2006. gada 11. aprīļa spriedums lietā Nr. 2005-24-01, para. 10.

[10] ECHR case of Sisojeva and Others v. Latvia, no. 60654/00. 15.01.2007.; ECHR case of Tatjana Slivenko and Others v. Latvia, no. 48321/99. 09.10.2003.

[11] J. Pleps, Pašaizsargājošās demokrātijas princips (The Principle of Militant Democracy). Jurista Vārds, vol. 51/52 (1317/1318), pp. 12-17, Dec. 2023.

[12] K.Fedorova and N.Tshuikina, “From “Oppressors” to “Oppressed”: Baltic Russian Post-Soviet Speakers in Search of a New Identity through Social Networking,” Regional Studies of Russia, Eastern Europe, and Central Asia, vol. 13(1), pp. 29–53, 2024.

[13] D. Bleiere, I. Butulis, I. Feldmanis, A. Stranga and A. Zunda, Latvijas vēsture. 20. gadsimts (History of Latvia. 20th Century). Rīga: Jumava, 2005, p.144.

[14] The Supreme Court of Latvia, 30.04.2013. Case no. SKA-172/2013, A42945009, para.19.

[15] Satversmes tiesas 2018. gada 29. jūnija spriedums lietā Nr. 2017-25-01, para. 20.

[16] The Supreme Court of Latvia, 16.02.2017. Case no. C30706512, SKC-26/2017.

[17] Administratīvās apgabaltiesas 2017. gada 2. janvāra sprieduma lietā Nr. A420261115, AA43-0189-17/8, para. 3.2.

[18] A. Vilks, A. Kipane, and A. Krivins. “Preventing international threats in the context of improving the legal framework for national and regional security,” Social & Legal Studios, vol. 7(1), pp. 97-105, 2024.

[19] The Supreme Court of Latvia, Case no. A420229620, SKA-88/2024 ECLI:LV:AT:2024:1105.A420229620.14.S, 05.11.2024.

[20] The Supreme Court of Latvia, Case no. A420209922, SKA-112/2024, ECLI:LV:AT:2024:1125.A420209922.7.S. 25.11.2024, para 18.

[21] T. Rostoks and K.E. Kanasta, “Foreign and Domestic Policy Implications of Latvia’s Reaction to Russia’s Aggression against Ukraine,” Journal on Baltic Security, vol. 9(2): pp. 5-28, Nov. 2023.

[22] National Electronic Media Council (Nacionālā elektronisko plašsaziņas līdzekļu padome), LĒMUMS Nr. 199/1-2 (18012000000723-2), 18.05.2023. Available: https://www.lmepadome.lv/jaunumi/params/post/4294691/latvijas-mediju-etikas-padome-uzskata-par-nesamerigu-nedemokratisku-un-biro [Accessed Mar. 19, 2025].

[23] Public Electronic Media Council, “Atzinums par 2024. gada 24. februārī LSM.lv publicēto “Cūku komiksu”” (Opinion on the Pig

Comic published on 24 February 2024 on LSM.lv), Nr. 6/6-3, 12.03.2024. Available: https://www.seplp.lv/lv/media/2022/download?attachment [Accessed Mar. 19, 2025].

[24] Editorial Board of Latvian Radio, "Vārda brīvības robežas sašaurinās" (The boundaries of freedom of speech are narrowing). 04.05.2024. Available: https://latvijasradio.lsm.lv/lv/par-mums/informacija-presei/?id=994 [Accessed Feb. 12, 2025].

[25] E.Levits, "Demokrātijai ir pienākums sevi aizsargāt" (Democracy has a duty to protect itself), Jurista vārds. Dec.2014.

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 311-316

Research on Artificial Intelligence Platforms with the Possibility of Application in Diplomatic Activities

Plamen Teodosiev
Department of National Security, Faculty of Information Sciences, University of Library Science and Information Technology
Sofia, Bulgaria
p.teodosiew@unibit.bg

Pavlina Nikolova
Department of National Security, Faculty of Information Sciences, University of Library Science and Information Technology
Sofia, Bulgaria
p.nikolova@di.mod.bg

***Abstract*— Diplomacy and diplomatic relations, which are an important means of conducting political relations between states, despite being subject to strictly conservative rules, are also influenced by the development of technology. Just as the invention of the telegraph triggered its widespread application in diplomatic correspondence, the development of digital technologies contributes to the improvement of channels and the reliability of communication, so the appearance of artificial intelligence will have an impact on diplomacy and diplomatic relations in general. The report analyses the regulatory framework, explores artificial intelligence platforms with opportunities for application in diplomatic activities and concludes with some conclusions about the risks and negative consequences of its use.**

***Keywords*— *AI platforms, Artificial Intelligence, Diplomatic relations, international relations, national identity, global and international security* .**

I. INTRODUCTION

Artificial intelligence leaves an imprint on almost every aspect of our daily lives, both personally and professionally. Its influence is becoming more and more tangible for the businesses, and the technologies that have emerged since the advent of the first models are becoming more and more numerous.

And it will continue to change its appearance. AI tools lead to productivity improvements, process transformations, cost reductions, and faster and easier identification of new growth opportunities.

In the article, we will show a few key examples that show how the business, respectively the diplomatic service, can benefit from AI, regardless of the sector in which it operates.

A. The effect of AI on the IT sector

Artificial intelligence has already taken an undeniable role in speeding up the workflows of IT specialists. Employees in the field use AI in development, but not only.

According to data from Statista for 2024, developers use AI tools for the following activities: writing code (82%), searching for answers to questions (67.5%), debugging (56.7%), documentation (40%), and more. [1]

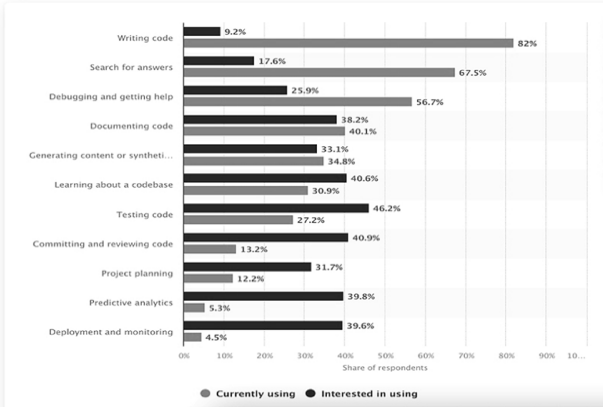


Fig. 1. Graph of programmers using artificial intelligence tools.

With the help of AI tools, data analysis is carried out, tasks and processes related to cybersecurity are optimized, as well as the management of the IT infrastructure and its maintenance.

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8500
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

All of this is possible thanks to AI's ability to analyze large volumes of data in real time. That is why people are able to act faster and be more informed.

In addition, the models we all have access to are also an opportunity to create "smart" applications. Thus, they can not only be controlled remotely and turn off heating when certain degrees are reached, for example, but also learn and make predictions so that they work autonomously.

B. Marketers and media experts, with application in public diplomacy

AI is already transforming the way we do marketing. With its help, content can be created much faster, advertising campaigns can be personalized and forecasts can be reached more efficiently based on the analysis of activities and the market.

The top 3 activities that marketers improve with the help of AI rank web content with the intention of searching for users – 84% of respondents to a Statista survey rely on these tools to improve the user experience, and 74% use them to increase their ranking in search engines. [1]

AI tools now have a place in headline writing, speeding up the content creation process – textual and visual - and helping more and more people claim a digital presence. However, this does not replace creativity and strategic approach in both marketing and media content, but only supports them.

C. Designers' work improved with AI

The market for generative AI in the field of design in 2023 reaches just over $550 million. By 2032, it is expected to reach nearly $8 billion, i.e. to grow by over 34% per year. [2]

This accelerated forecasted growth is due to the capabilities of generative AI to serve as a personal assistant in generating ideas, creating exemplary designs and drawing inspiration, there by significantly accelerating the design process.

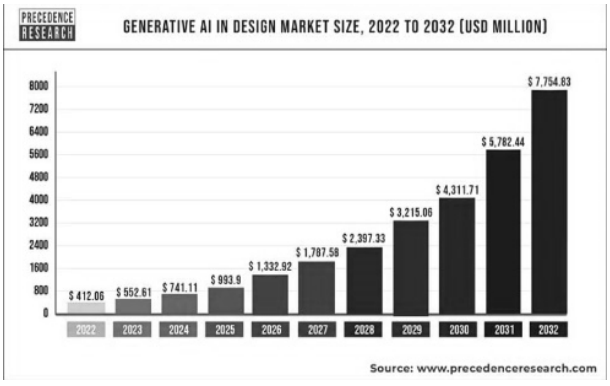


Fig. 2. Graphics of web designers using Artificial Intelligence.

In turn, this enables designers to work with more customers and gain a better standard. This applies not only to graphic, but also to web designers.

A study by hub spot shows that 97% of web designers have already used AI tools for the following tasks: generating images and media assets for sites (58%), creating web pages design (50%), experimental strategies and design elements (49%), improving designs (43%), tracking design quality (40%), auditing user experience (20%). [3]

This data undeniably proves the sensitive role of AI in the areas of design – not for the purpose of replacing designers, but to improve their efficiency.

By robotizing and automating processes, manufacturers can reduce the amount of repetitive tasks that are performed by humans, can improve production process schedules, and can even implement predictive and anticipatory maintenance, after analyzing historical data, to ensure a continuous and seamless production process.

We also present a few other areas where AI supports work in them:

- Areas such as AI-supported healthcare and finance.
- The effect on AI-supported education.
- The future of AI-supported call centers.

The implementation of artificial intelligence in all areas of activity is inevitable. This is due to the fact that AI tools are extremely affordable. They are already part of our daily lives.

However, their use should not be an end in itself. When it comes to the implementation of Artificial Intelligence, there are several mandatory steps [4]:

- Identify the goals that the business wants to achieve with the implementation of AI.
- Analysis of current processes and identification of opportunities for optimization and automation.
- Selection of appropriate tools capable of performing the tasks to which they apply.
- Limited testing of AI solutions to validate the usefulness of their integration.
- Training and adaptation period for the team, which must learn to work with the specific tools, and to adapt to the modified processes.

II. MATERIALS AND METHODS

A. Tools for researchers based on Artificial Intelligence

As Artificial Intelligence grows, the scientific community is taking advantage of advanced technologies that are changing the way research is done and scientific sources are accessed. In this text, we will look at some of the main applications of AI in research and the search for scientific resources.

- A large language model (LLM) is a type of Artificial Intelligence (AI) program that can recognize and generate text, among other tasks. LLMs are trained on huge data sets - hence the name "large". LLMs are built on machine learning:

specifically, a type of neural network called a transformer model. [5]

- Claude - is a chatbot with Artificial Intelligence (AI) generation and a family of large language models (LLM) developed by the research firm Anthropic.[6]
- Generative AI for InDesign — Leading page design and layout tools for desktop and digital publishing. Publish everything from books and brochures to digital magazines, ebooks, and more. [7]
- The biggest benefits of using AI for knowledge management include easier knowledge sharing, a personalized user experience, and the ability to save time. Some of the best use cases of AI for knowledge management include setting up an internal search and retrieval system, creating content with a customized LLM model, and monitoring issues. Some of the best AI knowledge management tools on the market include Team-GPT, Shelf, and Document360 due to the training capability. [8]
- Consensus - A search engine that uses Artificial Intelligence to automatically extract and condense research findings. [9]
- Copyleaks - This Artificial Intelligence assessment tool can quickly and accurately analyze tens of thousands of standardized tests at the state, national and university level without bias or external influences. [10]
- IRIS.AI - Comprehensive Research Processing Platform: smart search and wide range of smart filters, reading list analysis, automatically generated abstracts, autonomous data extraction and systematization. [11]

B. Platforms based on Artificial Intelligence used in diplomatic activities

Artificial Intelligence is starting to play an increasingly important role in diplomatic activities, using different platforms for data analysis, communication, security and decision-making. While many of these technologies are still in the early stages of development or pilot phases, they show significant potential for improving diplomatic practices. Here are some AI platforms and technologies that are already used or could be used in diplomatic activities:

a) *IBM Watson*

IBM Watson [12] is one of the leading Artificial Intelligence platforms that can be used to process large volumes of data, analyze text, and retrieve insights. Watson's technologies are able to analyze the content of documents, media materials, and other sources of information in real time, helping diplomats get quick and accurate recommendations for action. Possible applications are the analysis of political events and trends and the possible prediction of future crises, especially

b) *Google Cloud AI*

Google Cloud [13] offers a set of powerful AI tools for natural language processing (NLP), machine learning, and big data analytics. These technologies can be used to collect and analyze information from a variety of sources, including news platforms, social media, and official sources, to help diplomatic officials understand current events and respond in a timely manner.

c) *Microsoft Azure AI*

Microsoft Azure [14] offers a wide range of AI services, including data analytics, machine learning, and natural language processing tools. Possible applications are the construction of chatbots to improve communication and service to citizens on consular matters, to analyze political and economic data and to possibly recommend important events in the country of residence in the interest of diplomatic activity.

d) *Palantir*

Palantir [15] is a big data analytics platform used by government and military institutions to analyze and interpret information. In diplomatic activities, the platform can be used to integrate data from different sources and retrieve insights that can support decision-making in complex international relations. The platform allows the analysis of geopolitical risks and crisis forecasting, as well as the collection of intelligence information from various open sources.

e) *Kai by Kasisto*

Kai [16] is an Artificial Intelligence platform specializing in chatbots and conversational systems at this stage mainly in the financial sector. This technology is useful for creating digital assistants that can answer questions and provide information in real time, which allows for automated consultations related to travel, visa issues, providing advice and information about countries, etc.

f) C3.ai

C3.ai [17] is an AI-powered enterprise solutions platform that offers data analytics, machine learning, and process automation tools. In diplomacy, this platform can be used to model different scenarios and optimize diplomatic strategies by analyzing global trends and events.

III. RESULTS AND DISCUSION

A. Possible areas of application in diplomatic activities

Artificial Intelligence (AI) is an increasingly important tool in many areas of public life, and diplomatic activity is no exception. In recent years, AI technologies have provided new opportunities to increase the effectiveness of diplomatic efforts, both in managing relations between countries and in strategic decision-making. Although diplomacy obeys strictly conservative norms and has traditionally relied on the human factor for analysis and decision-making, AI can play essential roles by facilitating and speeding up processes, making them more precise and efficient. In this context, we can look at several main areas in which AI can be integrated into diplomatic activities [18]:

a) *Analysis of normative documents and information about important events*

Diplomacy usually requires a quick reaction to changes in legislation and changes in the situation in individual countries. There are a huge number of documents, news, reports and public statements that require careful analysis. Often these data can be confusing or contradictory. By using AI, diplomats can extract key data and use it in the decision-making process. Platforms based on AI can identify key phrases, terms and sentiments in media releases and rank them by importance or relevance and thus provide guidelines for the response of diplomatic staff. Platforms can be used for social media monitoring and press.

b) *Forecasting of international relations*

Artificial Intelligence can be used to analyze trends and patterns in international relations. [19] By processing large volumes of historical data, AI can predict to some extent the future behavior of certain countries or international organizations to be used to make informed strategic decisions. Platforms can also be used to monitor economic trends and forecast possible economic crises in certain regions, thus drawing up strategies for the prevention of migrant flows.

c) *Optimization of diplomatic negotiations*

Diplomatic negotiations are a complex set of complex interactions where multiple interests must be taken into account and compromises sought. Artificial intelligence can be used to optimize these processes and assist diplomatic officials by simulating different scenarios and recommending strategies. AI, by analyzing past negotiations, social media reactions, and public attitudes, can predict the actions of negotiating parties

d) *Supporting public diplomacy*

Public diplomacy is critical to shaping the image of the state on the international stage. AI can help manage public relations by analysing media and public opinion responses to diplomatic initiatives and negotiations and thus assisting diplomatic staff on approaches to improving the image of the state. AI platforms can also be used for the automated generation of diplomatic and press releases, which can be adapted to the public's reactions;

e) *Automation of administrative and operational processes*

In addition to a representative and negotiating function, diplomatic officials have administrative and operational functions that fill most of their daily lives. AI can automate the processes of processing, categorizing, sending and storing documents. AI can be used to automate the processes for processing visa and consular information, verify data, and provide an automatic response to frequently asked questions, such as grounds, document requirements, etc.

In conclusion, artificial intelligence offers numerous opportunities and solutions for modernization and optimization of diplomatic activity - from prediction of international conflicts to optimization of diplomatic negotiations and automation of routine processes. While AI cannot completely replace human judgment and intuition, it can serve as a powerful tool to support decision-making, speed up processes, and provide new opportunities for innovation in negotiation processes.

B. Possible risks of the use of AI in diplomatic activities.

Artificial Intelligence provides significant opportunities, but at the same time it carries serious risks that can test the security, ethics and efficiency of diplomatic activity. [18] These risks can not only affect the quality of decisions made, but also violate basic principles of international law and international relations. Possible risks can be defined as:

a) *Suggesting incorrect or unethical solutions*

AI systems generally rely on algorithms that make analyses and predictions based on available data. The problem arises when these algorithms fail to capture important social, cultural or moral nuances that usually play an important role in diplomatic relations. In diplomatic activities, complex and sensitive issues are often encountered that cannot be solved by mathematical algorithms and models alone. It is possible that the solutions proposed by AI ignore human and moral values, violate human rights and misinterpret cultural differences and thus generate and later implement diplomatic strategies.

b) *Prejudice and discrimination*

One of the serious risks of the use of AI in diplomatic activities is that the algorithms on which they are based may contain built-in biases if the data on which they are trained contains inequalities or stereotypes. The basic systems train their models on large volumes of historical data, which may include prejudices against certain countries, ethnic and religious groups. This can lead to an underestimation of a particular country or region, which can be reflected in the negotiation process.

c) *Transparency and clarification of decisions*

Many of today's AI models, especially those based on deep learning, are “black boxes,” meaning that even algorithm developers can't always explain how the system arrived at the specific solution. In diplomacy, where transparency and logic are crucial, this can be a serious problem.

d) *Security threats and cyber attacks*

AI systems in diplomatic activities are vulnerable to cyber attacks and manipulations. “Malicious actors” can attack and compromise processes related to diplomatic communication and thus manipulate diplomatic relations or “falsify” recommendations or misinform analysis systems, which can lead to the wrong processing of sensitive data.

e) *Dependence on technology and diminishing human judgment*

Excessive reliance on AI for decision-making can lead to a reduction in the involvement of the human factor in

decision-making processes. This is especially dangerous in diplomatic relationships that require intuition, emotional intelligence, and judgment that AI cannot provide. As advanced as AI is, it cannot and does not possess the human ability to adapt quickly to critical and unpredictable situations common in diplomatic activities.

f) *Abuse of AI to manipulate public opinion*

Artificial Intelligence can be used to manipulate information and public attitudes by creating fake news, disinformation, or targeted impact on social media. States or non-governmental organizations can use AI to automate the creation and dissemination of fake news, which can distort public perception of diplomatic activity and lead to negative effects on international stability.

g) *Need for regulation and standardization*

One of the most serious risks is the lack of clear international standards and regulations on the use of AI in diplomatic activities. [20] This can lead to differences in the way AI is applied between different countries, which creates the potential for unequal use of the technology. A serious problem is the lack of a legal frame work for the use of AI in diplomatic activities, as well as differences in the regulations and standards for data processing.

IV. CONCLUSIONS

While creating economic opportunities, there are also significant risks. Although AI technologies have the potential to improve people's lives and services, they can also be used maliciously. One of the most important risks is the question of who will be responsible for any damage caused by shared information about new technologies. The growing role of technology companies and new issues focused on AI technologies are among the important issues of diplomacy in terms of the risks of its use. Currently, artificial intelligence has various applications in the military field as well. Its use in this area also has implications for national and international security, which is one of the important issues of diplomacy. Thei ncreasing development and use of autonomous drones, drones in armed conflicts, has an impact on the security architecture of countries, which can also lead to a change in the balance of forces and hence lead to security risks. The means using artificial intelligence are mainly produced by private companies. For this reason, non-state actors, inparticular terrorist organisations, also have access to them, which is a risk to national and international security. In this regard, the use of Artificial Intelligence in the military field is becoming one of the important issues for diplomacy. Today, this problem is being discussed at the UN level, trying to regulate the use of armed drones using Artificial Intelligence technology.

The following conclusions can be made from the report:

- Developments in information technology and the widespread use of Artificial Intelligence will also affect the diplomatic service. This calls for an expert assessment of possible application activities, definition of a regulatory framework and the development of a methodology for its application.
- A wide range of experts and professionals, both IT and diplomats with extensive experience and practice, should be involved in defining the framework and methodology for the introduction and application of Artificial Intelligence in diplomatic activities.
- In order to create a unified international framework, the problem of introducing Artificial Intelligence in diplomatic and intelligence activities should be discussed not only in scientific forums but also at the highest level - UN, NATO, EU, etc.
- In order to minimize the risks of the use of AI, awareness campaigns and training of employees should be conducted on the risks of misinformation and manipulation, leakage of sensitive information, cyber-attacks, etc.

ACKNOWLEDGMENTS

The Submission was prepared under a project entitled " Exploring the possibilities for the application of artificial intelligence in diplomatic activities", financed by the Scientific Research Fund of the Republic of Bulgaria, contract KP-06-H/90/1, 10.12.2024.

REFERENCES

[1] A data collection platform using artificial intelligence, [Online] Available: https://www.statista.com/statistics/1424709/ai-automation-use-cases-by-marketers-worldwide. [Accessed February 20, 2025]

[2] Artificial intelligence platform for collecting statistical data, [Online] Available, https://www.precedenceresearch.com/generative-ai-in-design-market, [Accessed February 20, 2025]

[3] A blog to collect information in which industries artificial intelligence is used at work: [Online] Available, https://blog.hubspot.com/website/web-designers-ai; [Accessed February 20, 2025]

[4] Page from published material on an online university for programmers and information technology, [Online] Available: https://ai.softuni.bg/application?utm_source=blog&utm_medium=main-sa-program&utm_campaign=industries-that-benefit-most-from-ai&utm_term=cta-3&utm_content=nov-14-24; [Accessed February 20, 2025]

[5] Explanation page for large language models, [Online] Available: https://www.cloudflare.com/learning/ai/what-is-large-language-model/, [Accessed February 20, 2025]

[6] Artificial Intelligence Tool: [Online] Availabl:e https://claude.ai, [Accessed February 20, 2025]

[7] AI editor: [Online] Available: https://www.adobe.com, [Accessed February 20, 2025]

[8] The way AI is being used in knowledge management is by enhancing the efficiency of information retrieval and personalization of responses, [Online] Available, .https://team-gpt.com/blog/ai-for-knowledge-management/, [Accessed February 20, 2025]

[9] AI Search Engine for Research, [Online] Available: https://consensus.app/, [Accessed February 20, 2025]

[10] Artificial intelligence tool for charity[Online] Available: https://copyleaks.com/, [Accessed February 20, 2025]

[11] Artificial intelligence search engine [Online] Available: https://iris.ai/#Main, [Accessed February 20, 2025]

[12] Artificial Intelligence Tool: [Online] Available: https://www.ibm.com/watson, [Accessed February 20, 2025]

[13] [Artificial Intelligence Tool: [Online] Available: https://cloud.google.com/products/ai, [Accessed February 20, 2025]

[14] Artificial Intelligence Tool: [Online] Available https://azure.microsoft.com/en-us/solutions/ai, [Accessed February 20, 2025]

[15] [Artificial Intelligence Tool: [Online] Available https://www.palantir.com/, [Accessed February 20, 2025]

[16] Artificial Intelligence Tool: [Online] Available https://kasisto.com/products/kai-platform/, [Accessed February 20, 2025]

[17] Artificial Intelligence Tool: [Online] Available https://c3.ai/, [Accessed February 20, 2025]

[18] "Artificial Intelligence and International Relations: A New Era of Diplomacy?" by Tim Stevens (International Affairs, 2018), Non-book and other formats;

[19] "The Role of Artificial Intelligence in Diplomacy and Geopolitics" by George Washington University (2019), ; Non-book and other formats

[20] M. Zahariev, Legal and Ethical Challenges from Copyright Perspective of Implementing Artificial Intelligence in Education. In: Conference Proceedings of the 14th International Conference The Future of Education, Hybrid Edition, Online Event 19 June 2024, in Florence (Italy) 20-21 June 2024 / Filodiritto Editore. – pp. 639-644. ISBN 979-12-80225-60-3. ISSN2384-9509. DOI 10.26352/I620_2384-9509

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 317-322

Joint Information System Model Appliance in Man-Made Crisis Management

Laila Vaivode
State Police College
Department of Humanity Science;
Business University "TURĪBA"
Riga, Latvia
vaivode.laila@gmail.com

***Abstract*- Several crisis communication models can be applied in the discourse of man-made crises occurrence, such as terrorist attacks, cyber-attacks, or explosions caused by negligence and other similar events. However, one of the most comprehensive models in practical terms- and yet one of the least scientifically researched- is the Joint Information System (JIS) model. By nature, the resolution of such critical incidents, which are driven by human intention and action, requires the involvement of multiple actors, primarily state security institutions, as well as non-governmental organizations and possibly others. The JIS model thus provides a collaborative framework for crisis communication, involving multiple stakeholders, including government emergency responders, media representatives, community leaders and other actors depending on the type of incident. The JIS approach subsequently ensures that critical information dissemination is coordinated, consistent and effective in addressing the needs of all involved parties. The JIS model is based on five key principles: 1) Integrated communication, which requires collaboration among all stakeholders to ensure a unified message development and delivery, 2) Audience-focused communication, which prioritizes understanding the concerns and informational needs of different audiences to tailor messages accordingly, 3) Timely and accurate communication, which ensures that stakeholders receive reliable and up-to-date information throughout the various crisis phases, 4) Credible communication, which focuses on building trust and maintaining the credibility of information sources and 5) Continuous communication, which highlights the importance of sustained information-sharing in the precrisis stage and throughout both the crisis management and recovery phases. Recovery from a man-made crisis, including but not limited to terrorist incidents, is a complex and multifaceted process that encompasses physical, emotional, social, and economic dimensions. In the aftermath of such events, effective communication is crucial for maintaining public safety, disseminating critical information and mitigating the psychological and social impacts of the crisis on affected areas and citizens. This paper examines the application of the JIS model in man-made crisis scenarios, analysing its effectiveness in ensuring structured and transparent communication. The research employs a qualitative analysis of past crisis events where the JIS model has been implemented, drawing insights from case studies and best practices that are available online. The findings indicate that the JIS model significantly enhances crisis response by fostering coordination among stakeholders, reducing misinformation and improving public trust, consequently- maintaining reputational aspects of the state authorities high, that is one of the cornerstones of the successful crisis management. Overall, the JIS model is a highly effective approach to crisis communication, particularly in the context of man-made crises. By adhering to its principles, organizations can enhance their crisis management capabilities, minimize the adverse impacts on affected communities, and facilitate a more efficient recovery process.**

Keywords*- *Crisis communication, Joint Information System (JIS) model, man-made crisis management by state governed security authorities.

I. INTRODUCTION

This study aims to evaluate the role of Joint Information System model in enhancing crisis response mechanisms, with particular attention to their potential applicability within the newly developing Latvian Crisis Management Centre. It investigates how JIS can improve communication, ensure inter-agency coordination, and enhance public trust during man-made crisis events. By analysing real-world implementations and established best practices, the study highlights the effectiveness of JIS and provides practical recommendations for its adoption, especially valuable for emerging systems still in development,

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8503
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

A critical finding of the research is the notable scarcity of academic literature focused specifically on JIS. Existing studies often address broader crisis management topics or focus on technological dimensions (e.g., IT systems), despite JIS being a pivotal component in state-led security and emergency responses. It is routinely applied in real-world incidents that involve multi-agency collaboration, such as police, fire brigades, and emergency medical services.

Though extensively used in countries such as the United States, Australia, Canada, and the United Kingdom, scholarly attention to JIS remains limited. Regardless of the size and number of state or federal agencies involved, the JIS model has consistently demonstrated its value in delivering accurate, timely, and coordinated communication across entities. Over decades, it has proven its utility in practical applications, even though it has rarely been the central focus of academic inquiry.

One key research observation is that the JIS model has been adopted globally and is recognized as an effective and practical tool in managing both natural and man-made emergencies. For this study, a comparative analysis was conducted across four countries-Australia, the USA, the UK, and Canada-each representing a multilayered emergency governance structure across three continents. Although it is difficult to trace the exact origins of JIS in each country due to limited historical documentation available publicly, its universal appeal and practical value suggest that the model either developed independently in response to operational needs or was informally adopted based on its effectiveness (ref.: TABLE 1.).

TABLE 1. JIS SIMILARITIES AND DIFFERENCES

Feature	**Australia**	**USA**	**UK**	**Canada**
Structure	Decentra-lised, state- led	Federal interven-tion possible	Centralised national control	Provincial-led, federal support
Incident Command System	AIMS	ICS (NIMS)	JESIP (JDM)	IMS
Use of JIS/JIC	Forest fires, flood, security incidents	Hurricanes wildfires, terror events	Security threats, public health crisis	Wildfires, floods, pandemics
Public informa-tion coordina-tion	SES, EMA, BoM, Police	FEMA, JIC's	JESIP, COBR	Public Safety Canada

A coordinated information system like JIS plays a vital role in modern crisis management by enabling:

a) *Rapid information sharing*, ensuring that real-time updates on crisis developments reach both responders and the public efficiently [5].

b) *Consistency and accuracy*, preventing rumours, misinformation, and speculation by maintaining a single, verified source of truth [6].

c) *Public trust and engagement*, enhancing compliance and reducing panic by communicating transparently, clearly, and effectively [7].

d) *Efficient resource coordination*, helping emergency services deploy personnel and materials strategically while also activating volunteer or NGO support when needed [8].

Without a structured communication system like JIS, crisis responses risk fragmentation, misinformation, public confusion, and operational inefficiency.

II. MATERIALS AND METHODS

Timely and coordinated communication is fundamental in any emergency response. JIS is not just a helpful tool, it is a structured, scalable framework for managing and disseminating information across all involved parties, including government agencies, stakeholders, media, and the public.

Case studies from the United States reveal how JIS has been successfully integrated into the National Incident Management System (NIMS). By enabling a synchronized flow of verified information, JIS helps prevent misinformation and supports unified decision-making—central to the ultimate goal of saving lives.

The purpose and importance of JIS. The core function of JIS is to ensure relevant, accurate, and real-time communication during emergencies (see *Fig. 1: Information Dissemination Model in JIS*). Whether the crisis involves natural disasters, cyberattacks, or public health emergencies, efficient communication can determine the success of the response and the level of public cooperation.

A. The role of Joint Information System in crisis management

Whether dealing with natural disasters, public health crises, or cyberattacks, effective communication plays a decisive role in determining whether a crisis is managed efficiently or escalates into widespread panic. The Joint Information System (JIS) allows agencies across various levels- local, regional, national, and federal- to collaborate seamlessly. This coordination ensures that accurate and timely information reaches both the public, who may still be at risk during the incident (e.g., in ongoing situations such as an "active shooter" scenario) and decision-makers within Joint Information Centre (JIC), where access to precise, up-to-date information is essential for informed and effective decision-making.

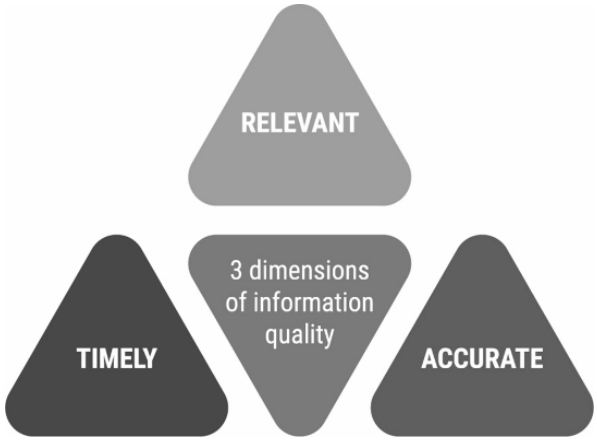


Fig.1. Information dissemination model in JIS.

By providing a centralized communication hub during multi-agency crisis responses, JIS significantly reduces the risk of confusion, misinterpretation, and misinformation, issues that frequently arise in complex emergencies. It ensures that messages are consistent, follow a unified strategy, and use standardized terminology, thereby avoiding contradictory statements that could hinder the crisis response and erode public trust. Maintaining public confidence is vital, as its absence can lead to reduced compliance in current and future emergency situations. Additionally, the system supports emergency personnel in making sound decisions based on real-time, verified data, ultimately strengthening the overall effectiveness of the crisis management process [9],[10].

Key Principles of JIS in Crisis Communication. JIS operates based on several core principles that ensure effective communication during emergencies:

- *Coordination and collaboration*: JIS promotes interagency coordination, even those under different ministries or jurisdictions, such as, emergency services, public health agencies, and law enforcement to share information and resources. This collaboration prevents duplication of efforts and ensures unified response. Importantly, it includes mechanisms for data protection and secure, controlled sharing of sensitive information and adhering to personal data protection rules.
- *Consistency in messaging:* one of the risk factors in crisis communication is possibility to operate with conflicting messages received from different agencies. To avoid public confusion, JIS ensures that all agencies use unified terminology and messaging strategies. This consistent communication is delivered across diverse platforms, including social media, to ensure clarity and avoid cognitive overload [11].
- *Timeliness and accuracy*: information in a crisis event must be rapidly disseminated while maintaining accuracy. JIS prioritizes real-time updates through multiple channels, which is especially vital for crisis managers at the different managerial levels and ensuring the public receives the latest developments, where possible, striving for even targeted message based on the community needs or territorial aspects of the incident.
- *Transparency and public trust*: keeping the public informed consequently fosters trust and compliance with emergency directives. Open communication reduces reliance also on unofficial sources and strengthens public confidence in official directives.
- *Flexibility and scalability*: JIS can be scaled up or down depending on the severity of the incident. It is flexible and adaptable to different crises, from local emergencies to national disasters as well as flexibility can be ensured by setting up the satellite or mobile centres as deemed necessary.

JIS as cross- Agency communication facilitator system. JIS comprises several structural and functional components:

- *Joint Information Centre (JIC)*: the JIC can be named as the central hub for coordinating public information efforts. It brings together Public Information Officers (PIOs) from multiple agencies to develop and distribute consistent messages. The JIC can operate physically being deployed on the spot or virtually, by coordinating and synchronising the content and delivering necessary messages depending on the crisis incidents' nature, manpower and other elements [12], [13].
- *Public Information Officers (PIOs)*: PIOs are responsible for gathering, verifying, tailoring and disseminating information to the media and public. These officials ensure that all messaging aligns with the overall crisis management strategy.
- *Interagency Briefings and Reports*: regular updates between all involved agencies ensures that all relevant actors have access to the latest information. Such briefings vary in frequency and length based on the stage of the incident. This prevents misunderstandings and allows for cohesive and coordinated decision-making.
- *Utilization of multiple communication channels*: JIS utilizes all available media-press, television, radio, websites, SMS alerts, and social platforms- to maximize outreach. The mobile messaging system is used in high-risk situations where are possible imminent threat. This ensures that messages reach diverse audiences effectively [14].

Real-world applications of JIS in crisis management. Historically the JIS has proven its effectiveness in various

high-risk situations, affecting safety and security of the society, including:

- *COVID-19 pandemic*: agencies like the FEMA, IMS and local health departments used JIS to coordinate public health messaging, ensuring consistent guidance on safety measures, vaccinations and response efforts.
- *Natural Disasters* (hurricanes, wildfires, earthquakes): in disasters such as Hurricane Katrina and California wildfires, JIS helped to streamline emergency alerts, evacuation orders and recovery updates, increasing solutions to ensure maximum safety [15].
- *Terrorism and security threats, including man-made crisis*: during events going back like the 9/11 attacks, JIS facilitated interagency communication between law enforcement, emergency responders, and governmental officials.

JIS remains one of the most practical, handy and effective tools for the crisis management as a process and interconnected communication aspects. The United Kingdom's JESIP (Joint Emergency Services Interoperability Principles) serves also as a model of publicly accessible training and decision-making tools. Dedicated website includes educational videos and structured communication guidelines (*see Fig. 2: Decision-Making Model in JESIP*).



Fig.2 Decision making model in JESIP [2].

Applying JIS Models to Man-Made Crises. Following from the above findings and conclusions, it is evident that JIS is particularly relevant to the management of modern man-made crises, including:

- *Industrial accidents* (e.g., chemical spills, factory explosions and other accidents), by ensuring that affected communities receive also timely evacuation orders and safety instructions, followed by the psychological and medical care when required [16].
- *Cyber-Attacks.* Nowadays, when the number of cyber-incidents has significantly grown and continue to increase, JIS appliance allows to coordinate messaging between cybersecurity agencies, businesses, and the public to manage data breaches and minimize reputational [17].
- *Terrorism related incidents.* The JIS in terrorism situations is crucial mechanism, as it allows rapid managing public safety communications while preventing the spread of misinformation and panic as well as causing secondary damages [18].
- *Misinformation/Disinformation campaigns.* Often underestimated, but yet crucial from the security threats perspectives, especially when intentional disinformation campaigns can be causing significant impact both in short and long terms. By applying JIS, is possible to eliminate or minimise harmful narratives during elections, pandemics, or social unrest through consistent, fact-based messaging and proactive community engagement [19].

In each scenario, the JIS helps to ensure that all involved organizations are aligned in their messaging and response efforts.

B. Crisis management centralisation effort in Latvia

Latvia has recently undertaken significant structural reforms to strengthen its national crisis response capacity, notably through the establishment of a centralized Crisis Management Centre (CMC). This institutional innovation reflects a strategic shift towards more integrated and streamlined crisis management, with particular emphasis on improved inter-agency coordination, enhanced civil-military cooperation, and more effective public communication during emergencies [20].

As of January 28, 2025, the Latvian Government approved a series of draft legislative acts to create the Crisis Management Centre. The Centre is envisioned as a centralized hub responsible for managing various types of emergencies, including both natural and man-made crises. In line with global best practices, the CMC's mandate includes not only strategic oversight and decision-making, but also the operationalization of transparent and timely information flows- core components of an effective Joint Information System.

Structure and Functionality of the CMC. The CMC will operate under the direct authority of the Prime Minister [20], functioning as part of the State Chancellery. Its primary responsibilities include:

a. *Strategic Coordination during nation-wide threats.* The CMC will provide centralized coordination of crisis responses at the highest level, overseeing and synchronizing governmental actions across ministries and agencies during large-scale emergencies.

b. *Civil-Military cooperation*. Recognizing the increasing complexity of modern crises, the CMC will serve as a liaison platform to ensure seamless collaboration between civil authorities and the armed forces.

c. *Public communication.* A major responsibility of the CMC is to guarantee accurate, timely, and transparent public communication during crises. This reflects a core principle of the JIS model and is vital for maintaining public trust and compliance with emergency directives.

A particularly notable development is the planned establishment of a Situation Centre (SITCEN) within the CMC. This 24/7 operational unit will facilitate continuous monitoring, threat assessment, and real-time information exchange in cooperation with responsible institutions. SITCEN's role will mirror the intelligence-sharing and coordination functions typically embedded within the JIS framework in other countries.

To ensure the effective functioning of the CMC, the Latvian Government is concurrently implementing key structural and legal reforms:

- *Restructuring of the Crisis Management Council*. The Council has been expanded to include all Ministers, thereby institutionalizing cross-sectoral decision-making during national crises and aligning with comprehensive governance models seen in other advanced crisis management systems.
- *Empowerment of the Crisis Management Board*. This Board is now authorized to issue binding directives to state institutions, municipalities, legal entities, and individuals during declared civil crises. It also holds the statutory authority to declare a state of emergency, thereby enhancing Latvia's legal readiness for extraordinary situations [21].

The establishment of the CMC presents a critical opportunity to integrate the JIS model within Latvia's evolving crisis architecture. Key synergies include:

- *Institutional alignments.* With its centralized communication and coordination mandate, the CMC is structurally well-positioned to host or lead a JIS-style platform, including the creation of a Joint Information Center (JIC) or equivalent unit.
- *Operational readiness.* The SITCEN's continuous monitoring and threat assessment functions could serve as a backbone for a national JIS, facilitating real-time information flow to decision-makers, responders, and the public.
- *Public trust and transparency.* Given JIS's proven success in enhancing transparency and trust in crisis communication, its implementation in Latvia would significantly reinforce the country's efforts to ensure cohesive and coordinated messaging in emergencies.

In summary, Latvia's centralization of crisis management through the creation of the CMC demonstrates a forward-thinking approach grounded in international best practices. By integrating the JIS model into this new institutional framework, Latvia can further bolster its resilience against complex emergencies, particularly those of a man-made nature, and ensure that both decision-makers and the general public are equipped with the accurate and timely information necessary for effective response.

CONCLUSIONS

This research paper, along with prior practices, clearly indicates that the Joint Information System (JIS), both as a technical framework and as a decision-making process, is a critically important component of modern crisis management. It ensures that information shared across crisis management agencies is accurate, timely, and coordinated. By promoting collaboration, consistency, transparency and scalability, the JIS reduces confusion, builds public trust, and facilitates more effective emergency responses.

Mechanisms such as the Joint Information Center (JIC) and the role of Public Information Officers (PIOs) contribute significantly to streamlining communication between emergency management institutions and the public. These mechanisms enhance the overall responsiveness and resilience of crisis management efforts. As crises evolve in complexity, especially with the rise of hybrid threats, which are now more than just a theoretical concern, the role of JIS remains indispensable throughout all stages of crisis management: from the pre-crisis phase, through incident response, and into post-crisis recovery.

In light of these findings, it is important to emphasize that the establishment and ongoing development of Latvia's Crisis Management Centre (CMC) represents a major step forward. It reflects a clear commitment to advancing toward a joint European Union security management concept [22],[23],[24]. Within this framework, there is a strong need to develop and maintain a robust yet adaptable JIS model.

However, as Latvia embarks on this path, several challenges must be carefully addressed and prioritized-especially when considering JIS within the context of man-made crises:

- Data security and protection.
- Interoperability of systems already in use across various crisis management institutions [20].
- Legislative and administrative alignment.
- Public trust, reputational and ethical considerations.

Given that the Latvian CMC is still a relatively new institution and that it is expected to assume responsibilities not commonly centralized in other countries, such as enhanced civilian-military cooperation, there is significant scope for further research. Key areas for future study include:

- Integration of Artificial Intelligence (AI) and Big Data into the JIS, potentially leveraging models already developed within the European Union [25].
- Strengthening cross-border cooperation also in crisis communication and response aspects.
- Expanding public-private partnerships in the domain of security related emergencies.
- Enhancing training and capacity-building, including preparation for civil defence aspects.

In conclusion, the effective integration of the JIS into Latvia's evolving crisis management structure is not only a national priority but also a critical contribution to the broader European security architecture. It requires both strategic vision and ongoing adaptation to meet the dynamic challenges of today's threat landscape.

REFERENCES

[1] U.S. Department of Homeland Security, "National Response Framework," 4th ed., Oct. 2019. [Online]. Available: https://www.fema.gov/sites/default/files/2020-04/NRF_FINALApproved_2011028.pdf. [Accessed: Mar. 17, 2025].

[2] JESIP, "The Joint Decision Model (JDM)," 2025. [Online]. Available: https://www.jesip.org.uk/joint-doctrine/the-joint-decision-model-jdm/. [Accessed: Jan. 23, 2025].

[3] T Federal Emergency Management Agency, "National Incident Management System," 3rd ed., Oct. 2017. [Online]. Available: https://www.fema.gov/sites/default/files/2020-07/fema_nims_doctrine-2017.pdf. [Accessed: Feb. 17, 2025].

[4] European Commission, "EU Civil Protection Mechanism," Feb. 2025. [Online]. Available: https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/eu-civil-protection-mechanism_en. [Accessed: Jan. 20, 2025].

[5] Federal Emergency Management Agency, "NIMS Basic Guidance for Public Information Officers," Dec. 2020. [Online]. Available: https://www.fema.gov/sites/default/files/documents/fema_nims-basic-guidance-public-information-officers_12-2020.pdf. [Accessed: Feb. 17, 2025].

[6] National Response Team, "Joint Information Center Model," Apr. 2013. [Online]. Available: https://www.nrt.org/sites/2/files/Updated%20NRT%20JIC%20Model_4-25-13.pdf. [Accessed: Feb. 20, 2025].

[7] Pennsylvania Department of Health, "Joint Information System (JIS) and Joint Information Center (JIC)," 2016. [Online]. Available: https://www.pa.gov/content/dam/copapwp-pagov/en/health/documents/topics/documents/emergency-preparedness/Joint%20Information%20System%20and%20Joint%20Information%20Center%20-%20FEMA.pdf. [Accessed: Feb. 17, 2025].

[8] Federal Emergency Management Agency, "National Incident Management System," 3rd ed., Oct. 2017. [Online]. Available: https://www.fema.gov/sites/default/files/2020-07/fema_nims_doctrine-2017.pdf. [Accessed: Feb. 17, 2025].

[9] B. Van De Walle, M. Turoff, and S. R. Hiltz, *Information* Systems for Emergency Management. New York: M.E. Sharpe, 2010.

[10] J. C. Pine, Technology and Emergency Management, 2nd ed. Hoboken, NJ: Wiley, 2017.

[11] L. Vaivode, S. Ammar, "The role of social media during and in the aftermath of a terrorist attack," Acta Prosperitatis. *Journal of Turiba University*, no. 10, pp. 131-144, 2019. [Online]. Available: https://www.turiba.lv/storage/files/10-acta.pdf. [Accessed: Jan. 24, 2025].

[12] Sacramento County Office of Emergency Services, "Joint Information System Annex," Jun. 2019. [Online]. Available: https://sacoes.saccounty.gov/EmergencyManagement/Documents/Planning/JIS%20Plan%202019%20FINAL.pdf. [Accessed: Feb. 10, 2025].

[13] M. T. Kimour and D. Meslati, "Deriving objects from use cases in real-time embedded systems," Information and Software Technology, vol. 47, no. 8, p. 533, Jun. 2005. [Abstract]. Available: https://doi.org/10.1016/j.infsof.2004.10.003. [Accessed: Feb. 10, 2025].

[14] N. L. Le, J. Zhong, E. Negre, and M.-H. Abel, "CORec-Cri: How collaborative and social technologies can help to contextualize crises?" arXiv preprint arXiv:2310.02143, Oct. 2023. [Online]. Available: https://arxiv.org/abs/2310.02143. [Accessed: Feb. 12, 2025].

[15] Idaho Transportation Department, "State of Idaho Joint Information System/Center Operations Plan," Boise, ID, 2012. [Online]. Available: https://itd.idaho.gov/pop/assets/JISOperations.pdf. [Accessed: Jan. 10, 2025].

[16] U. Začs, "Security risk and crisis management: Analysis of survey results," presented at the SECUREU Project Conference, Turība University, Riga, Latvia, Apr. 2023. [Online]. Available: https://security.turiba.lv/wp-content/uploads/2023/05/Ugis-Zacs-paper-03.04.2023.pdf. [Accessed: Jan. 17, 2025].

[17] M. Auziņš, "Risk and crisis management in higher education institutions: The experience of the University of Latvia," Latvian Higher Education in Crisis, Riga: University of Latvia, 2011.

[18] M. Auziņš, "Risk and crisis management in higher education institutions: The experience of the University of Latvia," Latvian Higher Education in Crisis, Riga: University of Latvia, 2011.

[19] U.S. Department of Homeland Security, "National Response Framework," 4th ed., Oct. 2019.

[20] Ministry of the Interior of the Republic of Latvia, "Minister of the Interior of the Republic of Latvia: We are ready to strengthen crisis management across the European Union," European Social Fund, Mar. 9, 2025. [Online]. Available: https://www.esfondi.lv/en/about-eu-funds/news/minister-of-the-interior-of-the-republic-of-latvia-we-are-ready-to-strengthen-crisis-management-across-the-european-union. [Accessed: Mar. 9, 2025].

[21] Crisis Management Centre, "Crisis management centre to be set under the direct authority of the Prime Minister," Institute of Emergency Management, Mar. 25, 2025. [Online]. Available: https://www.iem.gov.lv/en/article/crisis-management-centre-be-set-under-direct-authority-prime-minister. [Accessed: Jan. 24, 2025].

[22] European Commission, "Artificial intelligence applied to disasters and crises management," Luxembourg, 2021. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/b2762bac-b839-11ef-91ed-01aa75ed71a1/language-en. [Accessed: Jan. 10, 2025].

[23] ResearchGate, "CRISIS: A System for Risk Management," 2012. [Online]. Available: https://www.researchgate.net/publication/304197313_CRISIS_A_System_for_Risk_Management. [Accessed: Feb. 20, 2025].

[24] European Commission, "Civil Protection," Feb. 2025. [Online]. Available: https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection_en. [Accessed: Feb. 17, 2025].

[25] GINA Software, "SmartCAD - Computer-Aided Dispatch System," 2025. [Online]. Available: https://www.ginasoftware.com/products/smart-cad/. [Accessed: Feb.16, 2025].

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 323-327

Application of Deep Learning in Artificial Intelligence Systems for Cyberattack Identification and Prevention

Gergana Varbanova
Department of Information Technologies
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
g.varbanova@naval-acad.bg

***Abstract* — Cyberspace has been established as the fifth domain of warfare, alongside land, sea, air, and space. With the increasing complexity and frequency of cyberattacks, traditional security mechanisms are becoming increasingly inadequate, necessitating the integration of Deep Learning (DL) into cybersecurity. The capability of automated detection and prevention of cyber threats through the analysis of large volumes of data, anomaly identification, and attack prediction—threats that would otherwise remain undetected by conventional security systems—plays a crucial role in ensuring cyberspace security. Deep neural networks, such as Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, and autoencoders, are instrumental in analyzing network traffic and user behaviour, enabling the early identification of cyberattacks. Deep learning can also be applied to automate incident response mechanisms. The high-speed analytical capabilities and self-adaptive nature of these models allow for dynamic cybersecurity defenses, including the autonomous blocking of malicious traffic, the identification of compromised systems, and the reduction of response time. Generative Adversarial Networks (GANs) further enhance security by simulating potential cyberattacks, thereby enabling the testing and refinement of defense strategies. However, these same networks can also be exploited for adversarial purposes, such as manipulating input data to deceive AI-driven cybersecurity systems, leading to incorrect classifications or attack predictions. Deep learning represents a transformative advancement in cybersecurity, offering intelligent, automated, and proactive solutions to combat evolving cyber threats. The continued development of adaptive AI-driven security systems will play a pivotal role in enhancing cyber resilience and safeguarding critical infrastructure against emerging cyber threats. The article examines the role of deep learning in cybersecurity, integrating technological aspects and the legal framework of the European Union (GDPR, eIDAS, AI Act) while analyzing the dual-use risk associated with generative adversarial networks (GANs). The emphasis is placed on the significance of biometric data and the necessity of human oversight, as excessive reliance on automated algorithms may lead to a false sense of security and discriminatory effects.**

Keywords*— *Artificial Intelligence, Cybersecurity, Deep Learning, Generative Adversarial Networks

I. INTRODUCTION

Cyberspace constitutes a powerful resource that provides swift and convenient access to information; however, it has also emerged as the fifth domain of warfare. The advancement of technology has led to its increasing use as a medium for orchestrating attacks aimed at undermining national security and compromising elements of critical infrastructure. Simultaneously, artificial intelligence (AI) systems are experiencing a surge in innovation, and their integration into security and defense is becoming increasingly crucial for analyzing, preventing, mitigating, and countering cyberattacks that target national security or transnational organizations.

For the purposes of this study, it is essential to define the concept of "artificial intelligence," which, in theoretical terms, is understood as the capability of computers or other machines to perform tasks that require human intelligence and rational behaviour—i.e., for a machine to be recognized as simulating human behaviour.

With the adoption of Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), a legal definition of the term "AI system" was established. It is defined as a machine-

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8490
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

based system designed to operate with varying levels of autonomy and capable of exhibiting adaptability after deployment. Such a system, either explicitly or implicitly, generates outcomes—such as predictions, content, recommendations, or decisions—based on the input data it processes, which may subsequently impact a physical or virtual environment.

The European Union's efforts are directed not so much at harmonizing and developing a common policy for building AI systems in specific key sectors [1] as at establishing regulations and imposing limitations on the application of AI where such systems affect fundamental human rights and may lead to their restriction.

Meanwhile, China and the United States have developed clear policies regarding the funding and integration of AI without imposing an overly restrictive regulatory framework. This, in turn, has concentrated high-tech companies and their resources within their respective territories.

II. Materials and Methods

This study employs the comparative legal method to examine the existing European Union legal framework governing artificial intelligence and its role in cybersecurity. The aim is to identify common principles, key differences, and potential gaps in the current legislation.

Additionally, a comparative analysis is conducted on European legal instruments such as the eIDAS and AI Act, focusing on provisions related to personal data protection, biometric technologies, and AI applications in cybersecurity.

The study explores the role of deep learning in cybersecurity, examining models such as Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, Autoencoders, and Generative Adversarial Networks (GANs). These techniques are analyzed in the context of cyber threat detection, automated incident response, and attack simulation. The discussion further considers the legal and ethical challenges surrounding AI-driven cybersecurity, particularly in relation to data protection, algorithmic bias, and regulatory compliance.

III. Results and discussion

In the context of cybersecurity, the development of AI-based systems raises the question of their application as part of defense mechanisms aimed at mitigating the consequences of cyberattacks, including the reduction of material damage to critical infrastructure that is essential for security.

An increasingly significant aspect of cybersecurity is the so-called Defense-in-Depth (DiD) approach, which is based on the concept of constructing multi-layered defense mechanisms [2] through the implementation of Deep Learning (DL) techniques.

The use of deep learning is of critical importance for defense, including in the maritime sector [3], which has also been targeted by cyberattacks in recent years. The vulnerability of various sectors of public life and security generates substantial financial losses, which increase exponentially on an annual basis.

From financial fraud facilitated by social engineering techniques to the disruption of critical infrastructure—such as the energy grid, the maritime sector [4], financial institutions, governments, and supranational organizations—all remain potential victims of cyberattacks.

Deep learning represents an advanced methodology in the field of machine learning, significantly enhancing the automation and precision of data analysis. A key component of deep learning is innovative artificial intelligence (AI) systems, including deep neural networks (DNNs) and recurrent neural networks (RNNs) [5],

Without delving into the technical aspects of the technology, which are beyond the scope of this study, its application in cybersecurity is of paramount importance for identifying sophisticated attacks that are difficult to detect using traditional security systems. These conventional systems often require constant human oversight.

DNN systems enable continuous monitoring and analysis of network traffic, allowing for the detection of anomalous user behaviour, which may indicate potentially malicious activity.

Another type of artificial neural network is the generative adversarial network (GANs), whose primary application is attack simulation. This process significantly supports cybersecurity experts in developing effective defense strategies. By simulating realistic cyberattack scenarios, GANs contribute to the enhancement of early detection methods and countermeasures against malicious actions, as well as the identification of anomalous behaviour in cyber incidents that do not result from human intervention.

AI systems are a valuable resource in processing unstructured and large-scale data, as well as in their automated analysis. This includes the examination of text, images, and behavioural patterns, which, through network analysis, can help identify attacks such as social engineering (phishing), distributed denial-of-service (DDoS) attacks, and other cyber threats.

Prioritizing legislative activity, including criminal law norms, should not come at the expense of technological solutions for cybersecurity protection. Effective analysis, counteraction, and mitigation of cyberattacks require a combination of legal regulation [6] with the implementation of appropriate security systems as well as ensuring the quality of data used in deep learning (DL).

The quality and volume of the data used are critical factors, as inadequately selected input data may lead to erroneous or unpredictable results. To ensure ethical, lawful, and technologically sustainable cybersecurity, Article 10 of the Artificial Intelligence Act establishes imperative requirements concerning training, validation,

and testing data for high-risk AI systems, including those in the field of cybersecurity. This regulation aims not only to enhance the transparency of neural networks, whose interpretability and reliability pose challenges in critical areas such as energy, medicine, and maritime affairs, but also to address specific risks in the cybersecurity domain. To ensure precision and reliability, it is essential to combine deep learning with verification methods, ethical oversight, and an interdisciplinary approach to the validation and analysis of output data.

The process of verification and subsequent control of output data prevents potential false positives, inaccuracies, and distortions in models, which may compromise security mechanisms against cyberattacks or trigger defense protocols due to incorrectly identified behavior as a threat. Additionally, data must be aligned with the specific application of the AI system and reflect the geographical, behavioral, and functional characteristics of the environment in which the high-risk DL system will be deployed. This is critical for preventing incorrect or biased conclusions, which could lead to adverse consequences for security and society.

In the context of cybersecurity, despite significant advancements in the use of artificial intelligence and deep learning, the human factor remains crucial for the effective management of these technologies. While AI accelerates data processing and automates incident response [7], its judgment does not always account for context, necessitating expert oversight. Over-reliance on algorithms creates a risk of a false sense of security, particularly in cases of attacks aimed at manipulating the model. Effective cybersecurity requires a balanced approach in which AI assists but does not replace human expertise.

If deep learning systems rely on incomplete or inaccurate data, the algorithm may block legitimate traffic or fail to identify and prevent an actual cyberattack. Ensuring the security of training data is of particular importance, as such data can themselves become the target of malicious interference aimed at altering and destabilizing the operation of the respective deep learning system. Finally, one of the most serious risks is the excessive trust cybersecurity experts place in algorithms, which may lead to the oversight of unconventional cyberattacks that AI is not trained to detect but could be identified as anomalies by a human analyst.

In the context of cybersecurity, predictive systems based on artificial intelligence (AI) and deep learning play a crucial role in the prevention and management of cyber threats. Their primary objective is the timely identification of threats and the prediction of their potential consequences before any damage is inflicted on an information system or critical infrastructure. These AI-driven systems overcome the limitations of traditional security mechanisms, which primarily rely on predefined rules and databases of known attacks. However, this approach often proves ineffective against emerging threats, including zero-day attacks.

In the field of cybersecurity, predictive models are of paramount importance, as their algorithms possess the capability for dynamic adaptation to the evolving cyber environment. For instance, if a predictive AI system detects anomalous behavior—such as a sudden increase in requests from a particular IP address or attempts to access secured systems—it can automatically block malicious traffic, activate additional authentication measures, or notify a cybersecurity expert for further analysis. The interaction between predictive AI systems and human expertise is essential, as it enables the reduction of response time and minimizes the risk of compromising critical systems.

The integration of predictive AI systems based on deep learning into critical infrastructure represents a significant advancement in cybersecurity. These technologies not only enhance early attack detection mechanisms but also transform the security paradigm, making it predominantly proactive rather than merely reactive.

Undoubtedly, artificial intelligence (AI) systems based on deep learning play a crucial role in cybersecurity [9]. However, these same technologies can be utilized not only as a defensive mechanism but also as a means of executing complex cyberattacks. This dual nature of AI algorithms presents significant challenges to cyberspace security and necessitates the development of advanced countermeasures.

Traditional cyberattacks rely on pre-programmed scripts and techniques such as phishing, social engineering, and Distributed Denial-of-Service (DDoS) attacks. The integration of AI-driven systems into this domain has led to the emergence of more autonomous, faster, and harder-to-detect cyberattacks. AI algorithms not only enable the identification of new vulnerabilities in real time but also facilitate their exploitation before they are detected and mitigated.

Particularly concerning is the use of generative neural networks, which can create highly convincing fake messages, deepfake images, and video content. These technologies can be leveraged to destabilize social groups, manipulate public opinion, or compromise the reputation of public figures. As a result, there is an increasing need for more sophisticated methods to detect AI-generated content and the development of effective counterstrategies against AI-powered cyberattacks.

One of the most effective cyberattacks facilitated by artificial intelligence systems is advanced phishing. In this method, the algorithm analyzes the social profiles of the targeted individual, examining their behavior and generating personalized messages that appear entirely authentic.

The expansion of deepfake technologies has led to their increasing application in the creation of fraudulent audio and video content, which can be used to manipulate targeted groups or specific individuals. Deepfake content is increasingly employed as a tool of social engineering, particularly in the context of financial fraud, resulting in significant financial losses on a global scale.

Another significant aspect in the development of artificial intelligence (AI) and deep learning systems is the use of biometric data. Numerous companies employ fingerprints and facial recognition to manage access to key corporate resources, yet the collection and processing of such data is a process governed by statutory regulations [8]. Biometric data are highly sensitive and fall under a special category of data subject to stringent legal protection throughout all Member States of the European Union. The fundamental principles and requirements for collecting, storing, and processing personal data are derived from the provisions of the General Data Protection Regulation (GDPR), but they are further elaborated in Regulation (EU) No 910/2014 (eIDAS) and the Artificial Intelligence Act.

Pursuant to paragraph 14 of the Artificial Intelligence Act, biometric data may enable the authentication, identification, or categorization of natural persons, as well as the recognition of individuals' emotions. In the context of establishing an eID wallet, the use of biometric identification is permissible. The Act itself restricts profiling based on biometric data and the categorization of individuals according to emotional analysis conducted by AI systems and the results generated by such systems [11]. Thus, when biometric categorization serves only an auxiliary function, paragraph 16 of the Act allows social networks to employ filters that categorize facial or bodily features, enabling users to add or modify images or video content, given that such a filter cannot be employed without the primary service offered by social networks—namely, the online sharing of content. On one hand, this legislative provision appears logical, yet on the other, it presents a substantial risk associated with the use of deepfake content.

From a cybersecurity standpoint, deepfake technologies give rise to social engineering tactics, identity fraud, and falsified communications, targeting both individual citizens and organizations. Generating realistic yet fabricated video or audio materials can mislead users into adopting erroneous beliefs, undermining trust in the cyber domain and potentially compromising public order or specific individuals. The Act acknowledges that, in certain instances, there exists a risk of technical inaccuracies in AI systems intended for remote biometric identification, which may lead to biased outcomes and discrimination against specific categories of natural persons. The Regulation (i.e., the Act) permits a particular category of authorized processing of biometric data and categorization of individuals, namely when such authorization is linked to detecting, preventing, or investigating criminal offenses, provided that appropriate safeguards for the rights and freedoms of third parties are observed and in compliance with Union law—see Article 50 of the Artificial Intelligence Act. High-risk AI systems employed in cybersecurity and the protection of critical infrastructure warrant particular attention. Precisely due to their heightened importance, the Act introduces the so-called "human oversight" [12], enshrined in Article 14, which is of paramount significance for critical systems in order to avert automated decisions with unforeseeable outcomes and to ensure that human control is exercised throughout the entire period in which AI systems are in use.

Furthermore, AI-driven systems designed with malicious algorithms can scan networks and adapt to security mechanisms by automatically encrypting or modifying their code to evade detection. Such an attack is particularly dangerous, as it can operate without human intervention and spread exponentially.

Artificial intelligence systems can facilitate the detection of zero-day vulnerabilities. By analyzing large code bases, an algorithm can identify previously unknown weaknesses, which may subsequently be exploited before developers can address them, potentially enabling a cyberattack. This creates the possibility for the automated generation of zero-day exploits, significantly increasing the security risk for various systems.

As part of modern social engineering, fake social media profiles controlled by artificial intelligence systems can interact with targeted individuals in a manner that appears entirely authentic. As a result, the targeted victim is often deceived into disclosing personal or sensitive information or even initiating substantial financial transactions in favor of malicious actors.

In recent years, there has been a growing use of deepfake videos and audio messages, which can be employed to manipulate public opinion or interfere in electoral processes [10]. This type of attack is particularly dangerous in the context of regional destabilization and ongoing military conflicts, as it facilitates the spread of highly convincing disinformation, making detection and counteraction significantly more challenging.

IV. Conclusion

Ensuring a secure cyberspace is directly linked to the implementation of real-time monitoring through artificial intelligence systems based on deep learning, which can identify anomalies in network traffic and user behavior. This dynamic adaptability of algorithms significantly reduces response time and minimizes the impact of cyberattacks, allowing for timely intervention before attacks cause serious security breaches.

Despite the high efficiency of automated technologies, cybersecurity cannot rely solely on technological solutions. The human factor remains a crucial element in the protection process, as cybersecurity experts play a key role in monitoring, validating artificial intelligence system outputs, and making strategic decisions to counteract sophisticated threats.

Effective cybersecurity requires a balanced approach that integrates automation, human expertise, and a regulatory framework to ensure resilience against the increasing artificial intelligence driven threats.

REFERENCES

[1] S. Mircheska, "Perspectives for the Development of Artificial Intelligence: Security Dimension of Artificial Intelligence in the

Military Sector," *Security and Defense*, vol. 2, pp. 43-55, Dec. 2024. Available: https://doi.org/10.70265/ETNV6785

[2] V. Babanov, "Internals of Defense-In-Depth Strategy in Cybersecurity," *Security and Defense*, vol. 2, pp. 37-42, Dec. 2024. Available: https://doi.org/10.70265/PNEZ3158

[3] S. Lutzkanova, "The Regionalization of European Security and Defense Policies in the Maritime Domain: The Black Sea Case," *Pedagogika-Pedagogy*, vol. 93, pp. 208-216, 2021. Available: https://doi.org/10.53656/ped21-7s.18def

[4] B. Nikolov and D. Nikolov, "A scenario-based approach to cybersecurity training for seafarers," in *Proceedings of the International Association of Maritime Universities Conference 2024*, Massachusetts Maritime Academy, United States, 2024, pp. 385–390.

[5] R. Nishat, N. Arif, and A. Bajwa, "A comprehensive review of machine learning and deep learning applications in cybersecurity: an interdisciplinary approach," *Academic Journal on Science, Technology, Engineering & Mathematics Education*, 2024. Available: https://doi.org/10.69593/ajsteme.v4i04.118

[6] L. Lyubenov, "Domestic Legal Measures for Increasing Security in the Black Sea Region," *Security and Defense*, vol. 2, pp. 9-18, Dec. 2024. Available: https://doi.org/10.70265/VIRM1297

[7] V. Petrova, "A decision hierarchical model of cybersecurity risk assessment," in *Mathematics and Education in Mathematics*, Proceedings of the Fiftieth Spring Conference of the Union of Bulgarian Mathematicians, Burgas, Bulgaria, Sept. 2021, pp. 191-195.

[8] A. Kirkov, "Судебно-экспертная деятельность экспертов в Болгарии. Организация и проблемы," in *Цифровизация деятельности судов: текущие и перспективные задачи*, 2022, pp. 5-9.

[9] M. Oinonen and W. Morsi, "An Automated Wavelet Generation Tool for Cyberattack Detection in Substation Automation Systems," in *2024 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, 2024, pp. 512-517. Available: https://doi.org/10.1109/CCECE59415.2024.10667244

[10] R. Frick and M. Steinebach, "A Photo and a Few Spoken Words Is All It Needs?! On the Challenges of Targeted Deepfake Attacks and Their Detection," in *Proceedings of the 3rd ACM Workshop on the Security Implications of Deepfakes and Cheapfakes*, 2024. Available: https://doi.org/10.1145/3660354.3660357

[11] I. Nesterova, "Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance," *Information Polity*, 2022. Available: https://doi.org/10.3233/ip-211524

[12] L. eEnqvist, "'Human oversight' in the EU Artificial Intelligence Act: What, when and by whom?," *Law, Innovation and Technology*, vol. 15, pp. 508-535, 2023. Available: https://doi.org/10.1080/17579961.2023.2245683

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 329-340

Business Actions Posing Threat to National Security

Violeta Vasiliauskienė
Department of Management and Law, Faculty of Business
Kauno Kolegija Higher Education Institution
Kaunas, Lithuania
violeta.vasiliauskiene@go.kauko.lt

Anželika Banevičienė
Department of Management and Law, Faculty of Business
Kauno Kolegija Higher Education Institution
Kaunas, Lithuania
anzelika.baneviciene@go.kauko.lt

Vykintas Stumbrys
Department of Management and Law, Faculty of Business
Kauno Kolegija Higher Education Institution
Kaunas, Lithuania
vykintas.stumbrys@go.kauko.lt

***Abstract*—This paper explores how business activities can pose risks to national security, with a focus on Lithuania and the European Union. It analyzes how illicit practices, foreign ownership, and technological vulnerabilities contribute to threats in areas such as economic security, cybersecurity, and political influence. The research uses a qualitative approach, reviewing legal frameworks, national strategies, and real-world cases, including the revocation of UAB Foxpay's license and companies with ties to Russia and Belarus. These cases show how business links to authoritarian regimes, when left unchecked, can compromise critical infrastructure and sensitive data, or influence political decision-making. Technological advancements, such as artificial intelligence, digital finance, and global supply chains, increase vulnerabilities. Cases like Huawei and Kaspersky Lab illustrate the persistent risks of espionage, while supply chain attacks show how cyber threats can spread through business networks. The misuse of technology and lack of internal controls in some companies further exacerbate these risks. At the EU level, strategies such as the Security Union Strategy, the Digital Services Act, and the Chips Act aim to strengthen resilience, protect critical sectors, and regulate foreign influence. National measures, including Lithuania's investment screening and cybersecurity policies, complement these efforts by safeguarding strategic infrastructure and enhancing oversight. The study concludes that protecting national security in a digital and globalized economy requires a collaborative approach. Strong legal regulation must be combined with responsible business conduct. Security begins with knowing your partners and addressing indirect ties that may present risks. Ongoing legal development and consistent enforcement are essential to prevent business-related threats and maintain national stability.**

Keywords*— *economic security; national security; foreign influence; cybersecurity

I. INTRODUCTION

In an era marked by increasing geopolitical tensions, rapid technological advancements, and economic globalization, national security concerns extend beyond military and political dimensions to include economic, cyber, and technological threats. Business activities, while essential for economic growth, can pose significant risks to national security through illicit financial practices, strategic sector dependencies, cybersecurity vulnerabilities, and foreign influence. Recent cases, such as financial fraud in digital payment systems, supply chain cyber-attacks, and business ties with foreign entities that threaten state security, highlight the urgent need for stronger regulatory frameworks and oversight mechanisms.

The integration of artificial intelligence, digital financial transactions, and global trade networks has amplified the risks associated with economic security, making it imperative to assess how business actions influence national security. Governments, particularly within the European Union, have adopted legal frameworks and policies to mitigate these threats, but evolving challenges demand continuous adaptation and collaboration between regulatory bodies and businesses. Addressing these issues is critical to ensuring economic stability, protecting strategic sectors, and maintaining national sovereignty in a globalized world.

National security in Lithuania is a multifaceted concept encompassing several critical areas to ensure the country's sovereignty, stability, and resilience against various threats. One of the primary pillars is political security, which safeguards democratic governance, constitutional order, and the country's ability to independently conduct domestic and foreign policy [1]. Another essential area is military security, which focuses

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8505
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

on defence capabilities, territorial integrity, and cooperation with NATO allies to deter external aggression [2]. Additionally, economic security is important for maintaining stability, with an emphasis on protecting strategic industries, ensuring energy independence, and fostering economic resilience against external shocks [1, Art. 43]. Lithuania's social security involves efforts to strengthen national identity, social cohesion, and demographic sustainability, which collectively contribute to long-term national stability [1]. Cybersecurity measures aim to protect critical infrastructure, government networks, and sensitive data from cyber threats and espionage [1, Art. 37]. The areas of national security are closely related and the breach of one of them may have and has implications for other areas of national security.

The relationship between economics and national security is close and may not be evaluated separately. As A. L. Friedberg notes, "although the relationship may have grown more complex, economics and national security are and will continue to be intimately intertwined. Economic forces are changing not only the structure of the international system but the manner in which it functions. National security policy therefore may come to encompass measures designed to reduce a country's vulnerability to economic influence attempts as well as the more traditional forms of preparation for military defense" [3].

The aim of this study is to analyse specific cases where business activities pose threats to national security, highlighting their economic, technological, and regulatory implications. It seeks to examine the measures implemented at the European Union level to mitigate these risks, focusing on legal frameworks, cybersecurity policies, and economic controls. Additionally, the study evaluates Lithuania's national regulatory strategies, including investment screening, critical infrastructure protection, and measures to prevent illicit business influence on state security.

II. Methods and Materials

This study adopts a qualitative research methodology, focusing on the systematic examination of both national and European Union (EU) legal frameworks and strategic documents. It draws upon a wide range of regulatory texts, including binding and non-binding instruments from the European Commission, the European Parliament, and relevant Lithuanian legislative bodies. Additionally, the study incorporates national security reports published by the State Security Department of the Republic of Lithuania, as well as cybersecurity threat assessments issued by the National Cyber Security Centre. A critical component of the analysis is the review of selected Lithuanian business cases that have been publicly identified as posing potential threats to national security. These include, but are not limited to, cases involving violations of anti-money laundering (AML) and counter-terrorism financing (CTF) obligations, undisclosed ties with entities based in authoritarian regimes, and cybersecurity lapses in firms managing critical infrastructure. By triangulating these legal and empirical sources, the study aims to capture the evolving intersection between commercial activity, regulatory oversight, and national security imperatives in Lithuania within the broader EU legal context.

III. Results and Discussion

The relationship between EU measures on national security and those adopted by individual member states illustrates a complex balance between supranational coordination and national sovereignty. Through legislation, policy strategies, and judicial interpretation, the EU shapes the boundaries within which national governments may act.

Although national security remains primarily a competence of individual member states under Article 4(2) of the Treaty on European Union [4], the EU is increasingly involved in this area. This influence can be seen in sectors such as counterterrorism, cybersecurity, data governance, critical infrastructure protection, and foreign interference. Additionally, the Court of Justice of the EU strengthens the EU's role by ensuring that national security measures adhere to fundamental rights and the principles of the internal market.

The outcome is a legal and policy landscape in which national measures need to be carefully tailored to address both domestic security needs and EU legal obligations. This situation highlights the EU's significant influence in shaping security governance among its member states. The article offers a comprehensive analysis of the measures related to national security adopted by the EU and Lithuania.

A. EU measures against business threats to national security

At the EU level, Article 24 of the Treaty on European Union [4] and Article 72 of the Treaty on the Functioning of the European Union [5], which took effect in 2009, along with the Charter of Fundamental Rights [6], established the foundation for an EU security policy centred on the rule of law, fundamental rights, and solidarity. Member States are free to maintain law and order and safeguard states' internal security, whereas the EU's competence covers the Union's security [7, p. 646-647].

The EU has implemented policy, legal and technical measures to protect internal security while balancing economic interests and business operations. These measures cover areas falling under several EU strategies.

In July 2020, the EU adopted the Security Union Strategy for 2020-2025 to tackle a complex security landscape. This strategy emphasises a holistic approach that integrates various security policies. The strategy outlines key priorities for ensuring EU citizens' physical and digital security over five years. It focuses on priority areas where the EU can help Member States foster security. The strategy lays out the tools and measures to be developed to ensure security. It identifies four strategic priorities: fighting terrorism and organised crime, creating a future-proof security environment, building a strong security ecosystem, and addressing evolving threats [8].

Europeans' protection from terrorism and organised crime focuses on the significant threats posed by terrorism and radicalism, which destabilise society and endanger lives. Organised crime also incurs substantial economic losses, estimated to be between 218 billion and €282 billion annually [8, sec. IV (3)]. Key actions in the strategy include developing a counter-terrorism agenda and enhancing anti-radicalization efforts, improving cooperation with non-EU countries and international organisations, implementing plans against organised crime, migrant smuggling, drug trafficking [9], and firearms trafficking [10], reviewing legislation on asset freezing, confiscation, and environmental crimes.

The EU's new rules aim to combat money laundering and the financing of terrorism, enhancing detection and prevention measures for criminals within the financial system. Private sector operators must now conduct customer due diligence and report suspicious activities [11].

Additionally, Directive 2024/1260 on asset recovery and confiscation [12] will strengthen the fight against serious crime, enabling better confiscation of illicit profits. An upcoming directive on combating corruption will also harmonise penalties across the EU to address corruption risks [13].

Creating a future-proof security environment aims to establish safe and resilient critical infrastructure within the EU and protect against cyberattacks. Key actions include strengthening legislation on critical sectors, enhancing financial resilience, developing a cybersecurity strategy and joint cyber unit, promoting cooperation in safeguarding public spaces and addressing drone misuse [11].

The EU has implemented measures to protect critical infrastructure and enhance the resilience of essential services, notably through Directive 2022/2557 [14] and Directive 2022/2555 [15]. These directives address risks in key sectors such as energy, transport, banking, health, and public administration. Stress tests have been conducted in the energy sector to expedite the implementation of these directives.

A proposed Council Recommendation on a Blueprint setting aims for EU-level coordination against disruptions to critical infrastructure [16] and the Internal Market Emergency and Resilience Act (Regulation 2024/2747) [17] will help maintain market functioning during crises.

In collaboration with Member States and ENISA, the Commission has conducted a risk assessment of the EU's connectivity infrastructure and taken steps to improve the security of submarine cable networks essential for communication [11, p. 3]. The 5G Security Toolbox (2020) recommends mitigating telecom cybersecurity risks [11, p. 5].

The EU Cybersecurity Act [18] establishes a certification framework for ICT products and strengthens the EU Cybersecurity Agency (ENISA). The Digital Operational Resilience Act (DORA) [19] enhances the digital resilience of EU financial sector entities by updating existing rules amidst growing cyber threats. Directive 2022/2555 [15] expands cybersecurity requirements to all medium and large businesses across 18 critical sectors, introducing mandatory incident reporting and a European cyber crisis coordination structure. The Cyber Resilience Act [20] enforces mandatory cybersecurity measures for hardware and software, ensuring products are free of known vulnerabilities. The recently adopted Cyber Solidarity Act [21] creates a European Cybersecurity Alert System with Cyber Hubs for coordinated detection and response, supported by a Cybersecurity Emergency Mechanism and the EU Cybersecurity Reserve for significant incidents. The Digital Europe Programme allocates EUR 84 million for cybersecurity actions, including AI applications and post-quantum cryptography [11, p. 6].

The EU Network Code for cybersecurity rules related to cross-border electricity flows enhances system resilience in the energy sector [22]. The Wind Power Action Plan aims to improve the cyber-resilience of wind installations [23]. In transport, the Commission is advancing aviation and maritime security inspections [11, p. 2]. The Water Security Plan manual addresses measures against threats to water supply systems [24]. The revised EU Maritime Security Strategy [25] aims to protect critical maritime infrastructure from physical and cyber threats. A Common Information-Sharing Environment is being developed to improve information exchange among maritime authorities across borders and sectors [11, p. 3]. The revised Trans-European transport network Regulation [26] introduces new risk-proofing requirements for Member States to safeguard key transport infrastructure. In space, the EU Space Strategy for Security and Defence [27] includes actions to enhance resilience and further develop EU space-based dual-use services.

The EU Chips Act [28] is dedicated to strengthening supply chain security by reducing foreign dependencies in semiconductor supply chains. Meanwhile, the Critical Raw Materials Act [29] seeks to secure critical raw materials necessary for green and digital transitions, such as lithium and rare earth metals. This act focuses on diversifying supply chains and enhancing domestic extraction and recycling capacities.

EU Security Strategy emphasises that to build a strong European security ecosystem, EU governments, law enforcement, businesses, NGOs, and individuals must improve cooperation and sharing of information to combat crime and promote justice. Key actions include creating an EU 'police cooperation code,' enhancing Europol's role, linking Eurojust with judicial bodies, and strengthening ties with Interpol [8].

Artificial intelligence plays a significant role in law enforcement, but fundamental rights must be respected. While generative AI can aid cybercriminals in executing sophisticated attacks, Regulation 2024/1689 on Artificial Intelligence [30] aims to provide guardrails for

responsible AI use in the EU, ensuring the safety and rights of citizens.

The EU Security Strategy regarding tackling evolving threats includes addressing cybercrimes (like identity theft), illegal online content (such as hate speech), and hybrid threats (combining military and non-military activities). It recommends enforcing cybercrime laws and reviewing protocols on hybrid threats [8].

The European Economic Security Strategy [31] enhances the "whole of society approach" proposed in the EU Security Union Strategy by concentrating on protecting the EU, its Member States, and its citizens from economic threats. The strategy aims to achieve economic security by strengthening the EU's economic foundations and competitiveness, safeguarding against risks, and fostering partnerships with various countries to tackle common challenges. This approach will be essential for the EU's future security considerations.

Two key focus areas for economic security are combating market monopolisation and strengthening trade and economic defence.

Combating market monopolisation: Article 101 of the Treaty on the Functioning of the EU prohibits anti-competitive agreements, while Article 102 addresses the abuse of dominant positions. The EC Merger Regulation restricts concentrations that hinder competition [32, Art. 2 (3)]. Regulation 2022/2560 introduces measures to investigate foreign subsidies that distort the internal market [33]. The Digital Markets Act [34] and Digital Services Act [35] regulate tech giants to promote fair competition and prevent monopolisation.

Strengthening trade and economic defence: Regulation 2019/452 [36] enables screening of foreign investments that could threaten security or public order, allowing Member States to block or impose conditions on investments in critical sectors (e.g., energy, telecommunications, defence, etc.) [7, p. 648-650]. Regulation 2021/821 updates export controls on dual-use items, including emerging technologies and cybersecurity tools [37]. Regulation 2023/2675 protects EU businesses from economic coercion by non-EU states and permits trade restrictions against such countries [38].

The analysis of EU instruments demonstrates that they are continually being expanded and improved to address emerging challenges. Considering the Commission's unique role in safeguarding EU internal security, the Commission will undoubtedly provide new initiatives aimed at today's challenges.

2. *B. National measures against business threats to national security*

States employ different measures in order to protect national security from the threats caused by action of businesses.

The National security strategy of the Republic of Lithuania [1] foresees measures aimed at mitigating and removing risks that may be caused by the actions of business entities to national security. It foresees the following related tasks aimed at ensuring economic and energetic security of Lithuania:

1) to develop measures to encourage economic entities of the Republic of Lithuania to shift their business relations from authoritarian states to states that adhere to democratic values;

2) to develop the system of control of transactions and foreign investments in strategic sectors;

3) to reduce the dependence of Lithuanian transport sector from one country and increase diversification;

4) to increase control on import, export and transit of military equipment and dual-use goods;

5) to increase independence of Lithuanian electricity systems [1, Art. 43];

6) to ensure that the digitisation of the state through data opening, digital infrastructure, e-services, digital content or data creation, development and other digitisation initiatives is carried out in accordance with the interests of national security;

7) to ensure the safe use of new technologies for the state and society by employing only reliable equipment in critical information infrastructure and state IT resources; to implement AI, IoT, 5G, and digitalization following top cybersecurity and resilience standards, guaranteeing uninterrupted critical infrastructure operations during crises [1, Art. 37].

Protection of strategic sectors

The system of control of strategic sectors is foreseen in the Law on the Protection of Objects Important for National Security. The Law foresees measures to protect:

1) objects of strategic importance to national security (companies, installations and assets and economic sectors of energy, transport, information technologies and communications, other high technologies, finance and credit and military equipment);

2) assets and territory in protective zones;

3) strategically important cyber security objects [39, Art. 1].

It is foreseen that transactions regarding those objects should be protected from all risks to national security interests, the causes and conditions that give rise to such risks should be addressed. In particular, there is a list drawn up of such objects which are strategically important to national security. A risk assessment is carried out regarding such objects. The managing organs of companies of strategic importance to national security are prohibited from taking decisions that would contravene national security interests. Actions regarding companies in such a list (like reorganization, liquidation of assets and similar) are subject to approval by state institutions (national parliament or government). Investors are also vetted in order to establish their compatibility with national security interests. [39, Art. 6-

10]. One of the key criteria for assessing the compatibility of an investor or a party to a transaction with national security interests is the existence of past or present relations with foreign authorities, natural or legal persons of foreign countries that pose a risk or threat to national security [40]. Furthermore, the government may limit, stop or abolish contracts, investments or economic commercial activities [39, Art. 1]. There are requirements for persons who take up positions in governing bodies of strategically important companies [39, Art. 17].

The decisions are taken by the Coordination Commission for the Protection of Objects Important for National Security established by the Law. "The Commission is chaired by the Chancellor of the Government and includes representatives from various ministries, the Bank of Lithuania, the General Prosecutor's Office, the Police Department, the Special Investigation Service and the State Security Department" [41]. The subjects providing their opinions on the compliance with the national security interests are the Ministry of Foreign Affairs of the Republic of Lithuania, the Ministry of the Interior, the Police Department, the Prosecutor General's Office, and by request of the Commission - other bodies.

3. Restrictions of influence of business on politics

Speaking about business influence in politics, a tool to control the level of influence is the criminalization of influence peddling under Article 226, which serves as a safeguard against illicit business interference in political and administrative decision-making, thereby protecting national security interests [42, Art. 226]. This crime encompasses offering, promising, giving, or accepting bribes in exchange for using one's real or perceived influence over public institutions, officials, or international organizations to affect their lawful or unlawful actions. By penalizing such conduct, this measure upholds the integrity of public institutions, ensures transparency, and strengthens public trust in governance.

The transparency of influence of businesses and other entities on legislative processes is ensured by the regulation of lobbying in the Law on lobbying activity. The law indicates that persons aiming to influence politicians and their decisions need to register in the list of lobbyists and indicate in which area of legal regulation they aim to act. The lobbyist must complete a Transparent Legislative Declaration for each act that they aim to change and after the meeting with politicians. The Chief Official Ethics Commission keeps the list of the lobbyists and oversees their activities [43]. The information about lobbyists and all Transparent Legislative Declarations is public [44].

The regulation of the financing of political organisations also aims to limit the influence of business entities on political processes. According to the Law on Political Organisations of the Republic of Lithuania, businesses may not finance the political organisations, only donations from natural persons are allowed to finance the political campaign by their donations [45, Art. 19(1)(7)].

4. Ensuring cybersecurity of businesses

Specific measures are aimed at ensuring the resilience of business entities to cyber threats. National Cyber Security Centre of Lithuania (NCSC) pays special attention to cyber protection and resilience to threats in in organisations managing Critical Information Infrastructure [46, p. 12]. The Centre encourages such organisations to establish cybersecurity policy and implementing standards and other measures and monitors their progress regularly. In 2023 NCSC coordinated and carried out 17 thorough cyber security checks on such companies, together with the European Union Agency for Cybersecurity [46, p. 12].

The Centre also encourages other organisations to voluntarily adopt organisational and technical cyber security measures in their operations as they significantly reduce the risk of cyber-attacks, ensure business continuity for the organisation and reduce the damage caused by cyber incidents, thus minimising risks to national security that could arise [46, p. 12]

In order to ensure the resilience of organisations and companies, the NCSC carried out trainings and practical exercises in order to increase the ability of cyber security subjects to manage risks, to recognize cyber security incidents and react to them properly. In 2023, more than 11,500 people from public administration sector bodies, non-governmental organisations and small and medium-sized enterprises completed the various types of theoretical training organised by the NCSC [46, p. 37] In order to strengthen the resilience of the country's critical infrastructure to cyber threats, the NCSC, in cooperation with the US Naval Postgraduate School, organised for the first time the Industrial Control Systems Cybersecurity Course. The course was attended by 39 participants from Lithuania and Ukraine [47].

To effectively mitigate these risks, a collaborative approach combining strong state regulation with vigilant business practices is essential, ensuring appropriate measures are in place to protect economic and national security. As shown in examples, in an increasingly digital world, security begins with conscious efforts to mitigate risks. In both the business world and cyberspace, the key advice is to know service partners and the partners they work with. Enhancing legal regulation by the state is a must in these conditions

C. Case studies of businesses actions posing threat to national security

At their national level, states deal with influence in different fields. Here are cases discussed that reached courts and formed some precedents, and also cases that were presented by Lithuanian, Latvian, Estonian state security institutions. Authors also draw attention to the most known worldwide examples.

The relationship between economic factors and the threats businesses may pose to state security is a complex interplay. Economic security also serves as a foundation for national stability, and threats arising from business

activities can undermine state security, contributing to various vulnerabilities. Additionally, the interplay between technological advancements and security cannot be overlooked. As states increasingly rely on technology, the risks associated with cyber threats escalate, particularly as criminal enterprises exploit vulnerabilities in digital systems. Business activities may pose security threats, particularly when inadequate regulations lead to illicit practices, contributing to vulnerabilities that affect state security.

The role of state regulation is pivotal in mitigating these risks. As states seek to ensure their security, they must balance facilitating business operations with enforcing regulations that prevent illicit financial activities jeopardizing public welfare [48]. The lack of robust regulatory frameworks can lead to the proliferation of shadow economies and businesses operating outside legal boundaries, posing threats to economic security [49]. Inadequate regulation not only allows for financial crimes, such as money laundering and tax evasion, but also opens the door to corruption, further eroding public trust and state legitimacy [48]. In order to understand the nature of this relationship, some examples may be needed.

In the case of UAB Braitin (formerly UAB Lewben Investment Management), the company intended to acquire an investment company registered in Vilnius, UAB Prosperus Real Estate Fund II. In order to carry out this transaction, they needed the permission of state institutions. The Commission for Assessment of Compliance of Potential Participants with National Security Interests refused to grant such permission on the basis of information provided by the State Security Department of Lithuania (further – SSD). The SSD provided information to the Commission that the sole shareholder of the company had relations with individuals from non-EU and non-NATO countries that posed a risk to national security. Publicly available information provided by the SSD indicated that one of the persons was a suspect in criminal activity and was arrested in Belarus, and the other person, a businessman, had been under the EU sanctions for support, via his company, to the Lukashenko regime. [50, para. 12]. The threat had been addressed before becoming a breach of national security. The Vilnius Regional Administrative Court and Supreme Administrative Court of Lithuania upheld the authorities' decision, emphasizing that even minimal risks to national security justify state intervention over private business interests. The European Court of Human Rights also ruled that the company's rights had not been violated. It noted that while fair trial rights are important, they are not absolute—especially in cases involving national security where states enjoy a significant margin of appreciation. What matters is that the courts put in place enough safeguards to protect the interests of the company, even if some information had to be kept secret. [50, para. 60]

In another case, Lithuanian authorities raised national security concerns about a planned data storage facility that would connect to the Internet and local telecommunications networks, linking it to EU countries and Russia. The companies AmberCore DC and Arcus Novus which were registered at a technology park in Liepiškės near Vilnius. Arcus Novus was founded in 2003 and deals with the implementation and development of technological projects, including the transmission of information by satellite telecommunication. In 2009 Arcus Novus established a subsidiary company, later renamed AmberCore DC, which deals with the construction and development of data centres. The companies initiated a project to build a data storage facility near Vilnius, for which they required a permission from the abovementioned Commission for Assessment of Compliance of Potential Participants with National Security Interests. The permission was denied in 2016 due to the potential risks to national security. On the basis of report of SSD, the Commission indicated that Arcus Novus, through intermediary companies was owned and controlled by four citizens of the Russian Federation. The risk posed by Arcus Novus to Lithuanian national security was increased by the fact that "one of these owners, V.A., had previously worked in Russian companies directly linked with the Russian State and law enforcement authorities. Those companies "were overseen" by the Federal Security Service of the Russian Federation ("the FSB"). More specifically, from 2006 to 2009 V.A. had worked as a director of the Russian gas corporation's subsidiary company Gazprom Komplektacija in the Kaliningrad region, and from 2009 to 2014 had been the founder and deputy director of Gazinvest Group, another company operating in Kaliningrad and dealing in customs brokerage" [51, para. 10]. In Lithuania, the data storage facility was to be connected to the Internet and local telecommunications networks, linking it to EU countries and Russia. According to the SSD, this connection could enable Russia's FSB to access the facility through its intelligence centre, which conducts cyber spying against Lithuania, NATO, and the EU. The SSD warned that the FSB could intercept sensitive data, influence Lithuanian networks, use Lithuanian territory for cyberattacks, and, if key institutions became clients, disrupt the functioning of the State and its economy [51, para. 10]. As in the previous case, the threat had been addressed via legal and judicial means, by refusing permit for the planned activity. The Lithuanian courts upheld this decision, and the European Court of Human Rights found no violation of the companies' rights. It confirmed that national authorities had struck a fair balance between public interests and the companies' procedural rights, and that the use of some confidential material had not undermined the fairness of the hearing. [51, para. 117].

In another important case the Constitutional Court of Lithuania analysed the case involving the Lithuanian President committing severe national security breaches by unlawfully granting Lithuanian citizenship to J.B., a businessperson, in return for substantial financial and material support provided through his enterprises. J.B., through his business enterprises, provided significant financial and material assistance to the presidential campaign of the candidate for President in 2002. Such extensive financial backing created undue influence, allowing J.B. to leverage his enterprise's economic power for political advantage [52]. This created a

scenario where private enterprise interests directly influenced state decisions and presidential actions. This established a concerning precedent, demonstrating how economic power from enterprises could compromise governmental integrity, potentially exposing decision-making processes to external manipulation or foreign influence, thus directly threatening national security. The breach was addressed through the constitutional impeachment procedure, as defined in Article 74 of the Lithuanian Constitution. The Constitutional Court of Lithuania conducted an examination and concluded that the Lithuanian President had gravely violated the Lithuanian Constitution. This impeachment case exposed significant regulatory gaps in the national security framework, particularly concerning the intersection of enterprises and political power. It showed that there was no adequate conflict-of-interest prevention. The legal framework for preventing private enterprise influence or economic contributions from improperly affecting state decision-making was not sufficiently robust. To remove this gap, the legal regulation was changed, prohibiting enterprises from giving material support to politicians and political parties [52]. In addition, the Constitutional Court declared the President Decree on granting citizenship to the J.B. as unconstitutional [53].

In the case No. eI2-3776-1114/2024 [54], the national security breach was centered around the Lithuanian aviation company Aviabaltika, which was found non-compliant with Lithuania's national security interests. The breach occurred due to the company's long-standing commercial relationships and historical ties with entities from Russia and Belarus, countries officially considered hostile by Lithuania. Specifically, concerns were raised due to former shareholder and owner J. B., a Russian citizen with significant business ties to the Russian military-industrial complex, association with entities enhancing Russia's defence capabilities. Aviabaltika continued commercial activities involving entities from Russia and Belarus, including organisations directly involved in their military-industrial sectors, thereby indirectly supporting the strategic capabilities of adversarial states. Aviabaltika operated facilities within Kaunas International Airport's strategically important protection zone, a critical infrastructure site essential for Lithuania's national defense and security. The breach was directly addressed through formal regulatory actions. The Lithuanian Government, through the Commission on Coordination of Protection of Objects Important to National Security, conducted a thorough security review and declared Aviabaltika non-compliant with national security interests, effectively prohibiting further extension of the company's land lease within the critical security zone. The Vilnius Regional Administrative Court upheld the government's position, validating the proportionality and legitimacy of the security-based restrictions applied. The case revealed significant regulatory gaps regarding national security oversight. Existing procedures lack a proactive and systematic mechanism to monitor or review enterprises with sensitive foreign ties operating within national security zones. The regulatory framework did not clearly define how indirect or past ties with adversarial states should be assessed and at what thresholds they constitute a national security risk. Therefore, there is a need to clearly define regulatory criteria and thresholds specifying what constitutes unacceptable indirect business relationships or historical ties, ensuring consistent application across similar enterprise assessments [54].

Similarly, Supreme Administrative court case No. eA-393-520/2023 [55] shows that the Lithuanian Government and the National Security Coordination Commission determined that the enterprise seeking to expand its operations within a strategically sensitive security zone had ownership structures indirectly connected to individuals and entities affiliated with foreign state institutions, special services, and corporations closely related to the military-industrial complex of a foreign state, particularly Russia. A significant concern was the indirect control exercised by individuals associated with Russian state corporations, thereby creating vulnerabilities in critical national infrastructure protection due to potential foreign influence and espionage risks. Due to these foreign links, the enterprise's planned infrastructure expansion and reconstruction within the security-sensitive area adjacent to critical Lithuanian national security infrastructure was deemed incompatible with Lithuanian national security interests. The Lithuanian Government adopted a resolution based on the Commission's assessment, officially prohibiting the enterprise's planned activities (expansion and reconstruction) within the security-sensitive zone. The Supreme Administrative Court confirmed the government's decision as legitimate, proportional, and consistent with national security requirements. This case revealed that the existing regulatory frameworks did not clearly define how to monitor and transparently disclose foreign links or beneficial ownership in corporate structures, particularly when involving complex ownership chains and offshore entities. Therefore, there is a need to establish clear statutory definitions and objective criteria regarding the national security implications of indirect corporate ownership and beneficial interests, especially those involving entities or individuals affiliated with foreign state institutions or special services [55].

In another one case, the Vilnius Regional Administrative Court found serious threats to national security involved in a procurement contract between Lithuanian Airports and Nuctech, a Chinese enterprise, for the acquisition of baggage inspection systems — equipment integral to the operation and security of national critical infrastructure (airports) [56]. The main national security concern was that Nuctech was found to have ties to the Chinese government, including affiliations with Chinese military and intelligence services. This raised red flags about potential risks of surveillance, data interception, and system manipulation through hardware/software embedded in critical national infrastructure. By allowing a company with such affiliations to supply systems for airport security, Lithuania risked exposing sensitive data and operational

integrity to a foreign government with competing geopolitical interests. The Lithuanian Government took action to address the threat. An investigation was carried out by the Commission for Coordination of Protection of Objects of Importance to Ensuring National Security, which concluded that Nuctech's connections made it ineligible to operate within sensitive Lithuanian infrastructure. Based on these findings, the Government annulled the contract, citing national security grounds. The court upheld the Government's action, validating the national security rationale and procedural legality [56].

In the Vilnius Regional Administrative Court case No I-4964-764/2016 [57], the breach concerned potential threats to Lithuania's national security arising from the relationships between private enterprises and foreign state-affiliated entities. Specifically, UAB "FL Technics" was determined not to meet Lithuania's national security requirements due to its corporate association with AB "Avia Solutions Group", a company engaged in close commercial relations with Russian state-controlled entities. AB "Avia Solutions Group," the parent company of FL Technics, maintained significant commercial relations with the Russian state-owned enterprise "Rostec," whose CEO, S. C., was closely affiliated with Russian security services and sanctioned by the U.S. and EU for actions undermining Ukrainian sovereignty (specifically, Crimea's annexation). The association with S.C. and Rostec presented an indirect yet tangible risk of foreign intelligence influence due to S.C.'s known past involvement with KGB and high-ranking positions within Russian state structures. The identified national security risk was addressed by Lithuania's special commission, which is responsible for evaluating enterprises' compliance with national security interests. The Commission concluded in 2015 that FL Technics did not meet the required national security criteria, primarily because of its indirect ownership link to Russian entities considered hostile or detrimental to Lithuanian, EU, and NATO interests. This decision resulted in the Denial of the right for FL Technics to lease strategically important land within Vilnius International Airport. The decision revealed the lack of clarity in criteria defining connections that threaten national security (e.g., indirect ownership or commercial collaboration with foreign state enterprises). FL Technics challenged the criteria for being vague, unclear, and overly broad. Therefore, the court decision revealed the need to provide regulatory guidance clarifying what constitutes unacceptable national security risks stemming from corporate relationships or indirect ownership, specifying thresholds and conditions [57].

The Department of National Security of Lithuania likewise mentions example of such risks. The company operating in the transport sector had links with Belarusian companies – the state institute Belželdorprojekt and the company Želsviazprojekt BR. As part of the strategically important project, the company resumed contacts with the employees of these Belarusian entities and used them to carry out the tasks of the project, trying to hide it from the project developer. In this way, Belarusian entities gained access to information about the ongoing project and part of its engineering solutions. After the identification of the company's cooperation with Belarusian entities, its participation in strategically important projects was prevented. It is very likely that Russian and / or Belarusian entities, in order to interfere with the work of strategically important infrastructure facilities or obtain non-public information about it, will try to use cyber capabilities or take advantage of the vulnerabilities of personnel of strategically important companies [40, p. 71].

Almost all Lithuanian companies that previously cooperated with Russian Rosatom companies and their representatives did not break these ties. The main motives for cooperating with Rosatom are financial interests, opportunities to get jobs in projects carried out by Rosatom and the desire to maintain cooperation based on personal loyalty and friendship. Lithuanian companies with contacts with Rosatom, in order to participate in Ignalina atomic power station projects, use various tools, often act in a non-transparent manner and try to conceal the contacts they maintain, realizing that they are likely to be assessed as risky or threatening. The most popular ways of acting: creating a new name – setting up or acquiring a new shelter company; attempts to recruit specialists in projects by concluding individual contracts with them, who often try to conceal links with a company whose participation in the project would not be in the interests of national security. Lithuanian companies cooperating with Rosatom companies are not able to claim a large number of applications [40, p. 72].

The Latvian State Security Service notes that Latvian business cooperation with Russia to circumvent sanctions poses a great risk. Direct and indirect cooperation of local businesses with Russia remained the main source of risks to Latvia's economic security and international reputation. Security and other responsible services continuously assessed suspicious transactions by Latvian companies to detect and prevent violations of international sanctions. At the same time, Latvia continued to gradually move towards severing economic ties with Russia [58, p. 50].

It is likely that rapid development of AI and the wider-ranging use of the tools it provides have created a situation where national legislation and regulation have not been able to keep pace. Estonian National security report states that as such, easy access to ever more powerful resources is being accompanied by the misuse of AI: increasingly, false information is being spread through deepfake images, videos and audio clips, and large-scale, quick-learning language models are making it easier for cybercriminals to engage in social manipulation and phishing. In the last decade, the number of incidents involving the misuse of AI has increased and this trend is expected to continue in the near future, with the scope of incidents likely to grow as the quality of AI improves. Misuse of artificial intelligence appears in different ways. Use of deepfake in election campaigns in Poland and Slovakia was aimed to cause loss of trust in institutions. AI-generated image of an explosion near the Pentagon or similar spreads disinformation, deterioration in media literacy, reduced

threat perception. Use of deepfake to hold fake calls with Western politicians may cause loss of trust in institutions, undermining, influencing public opinion. Use of AI by Russia to produce disinformation aimed at loss of trust in institutions, influencing public opinion and outcome of elections [59, p 16].

Well known example of such a technological threat in 2020 is Huawei products related to the threat of espionage. Although Huawei has claimed that the Chinese government does not legally have the authority to compel it to build backdoors into its telecommunication system and that its subsidiaries and employees outside of China are not subject to the territorial jurisdiction of the National Intelligence Law, many legal experts have disputed this interpretation [60]. And a lot of countries even banned Huawei products in its institutions [61].

Some other examples of cybercrime-related cases revealing business vulnerabilities include a Moscow-based antivirus firm Kaspersky Lab was banned on the grounds of national security concerns. It is purportedly alleged that Kaspersky's products constituted a threat to national security and could be used to facilitate espionage by the Russian government [62, p. 279].

Over the past decade a long-term process of digitization of finance has increasingly combined with datafication and new technologies including cloud computing, blockchain, big data and artificial intelligence in a new era of FinTech. One of the recent and most highlighted cases in Lithuania was the Foxpay case. In 2024 Central Bank of Lithuania revoked the electronic money institution licence of UAB Foxpay for serious and systematic breaches of legal acts regulating the prevention of money laundering and terrorist financing, safeguarding of client funds and other legislation. Following the decision, Foxpay can no longer provide financial services. The Central Bank of Lithuania noted that Foxpay's operational shortcomings and breaches of legislation were identified in all areas inspected [63].

Foxpay infringed the following key requirements for the prevention of money laundering and terrorist financing (AML/CTF):

- Failed to ensure that its internal control system for AML/CTF was effective and sound. AML/CTF processes implemented in practice were not in line with internal procedures.
- Failed to ensure adequate identification of clients, their representatives and beneficiaries, including enhanced client identification.
- Failed to establish sufficient measures for monitoring client's business relationships and operations/transactions. Failed to ensure that clients' individual ML/TF risks were properly identified and assessed [63].

Allegations of money laundering, fraud and corruption dominated the narrative, and, pre-trial investigations led to the detention of seven individuals, including Ieva Trinkunaite, Foxpay's owner; her partner Vilhelmas Germanas; and Mindaugas Navickas, the husband of former Social Security Minister Monika Navickienė [64].

Examples of supply chain attacks attributed to state cyber capabilities made public in 2021: The French National Cyber Security Agency publicly accused the Sandworm group, which was affiliated with the Russian GRU, of carrying out attacks on the networks of French organizations in 2017-2020. The group gained access to the target systems by exploiting a vulnerability in software sold by the local IT company Centreon. The APT29 group, which was affiliated with Russian intelligence, which carried out a large-scale attack against the IT management systems manufacturer SolarWinds and its customers in 2019-2020, had launched a new supply chain attack campaign. It is likely that companies providing IT solution management services were chosen as the initial targets of the new attacks due to their access to their customers' information systems. The North Korean-backed Lazarus group's attacks were exposed, with the group carrying out malicious activities using software from South Korean and Latvian IT companies [58, p. 47].

In conclusion from these cyberspace related examples, states may consider new technological and legal vulnerabilities. 1. The reliance on emerging technologies such as blockchain, AI, and IoT in digital payments introduces new vulnerabilities that can be exploited by sophisticated attackers. 2. With lack of comprehensive legal frameworks to address the unique risks posed by digital payments, leaving gaps that cybercriminals can exploit. 3. Payment system security gaps, while used for bribery and money laundering, can cause significant moral and structural damage to societies and economies.

Concluding, all examples above we can state that technological advancements further complicate the landscape, increasing the potential for threats as companies face challenges in maintaining effective internal controls. Notable instances, such as the revocation of UAB Foxpay's license by the Central Bank of Lithuania for serious regulatory breaches, exemplify the repercussions of failing to uphold adequate regulations. Additionally, connections between companies and foreign entities, like those with Belarusian or Russian companies, pose risks by potentially compromising sensitive project information. Companies have been found to maintain ties with Russian state-operated entities, driven by financial interests and personal loyalties, despite the associated risks to national security. Businesses collaboration with Russia and China to circumvent sanctions presents a significant threat to economic security, and there is a continuous assessment of suspicious transactions to prevent violations. Cases like Huawei or Kaspersky Lab illustrate ongoing concerns regarding espionage and national security linked to technology firms. Supply chain attacks, attributed to state-backed cyber groups, reveal vulnerabilities exploited in the digital landscape.

To effectively mitigate these risks, a collaborative approach combining strong state regulation with vigilant business practices is essential, ensuring appropriate measures are in place to protect economic and national security. As shown in examples, in an increasingly digital world, security begins with conscious efforts to mitigate risks. In both the business world and cyberspace, the key advice is to know service partners and the partners they work with. Enhancing legal regulation by the state is a must in these conditions.

V. CONCLUSIONS

The relationship between business activities and national security is increasingly complex, with economic and technological factors playing a critical role in maintaining state stability. This paper shows that business actions—especially those involving critical infrastructure, foreign ownership, or influence in politics—can pose significant threats to national security. Lithuania has faced several real-world examples, such as the revocation of UAB Foxpay's license due to regulatory breaches and multiple cases involving business ties to entities from Russia and Belarus. These instances highlight how business interests, if unregulated, can compromise sensitive sectors and even influence political decisions.

Technological advancements further complicate the landscape, increasing the potential for threats as companies face challenges in maintaining effective internal controls. The growing use of artificial intelligence, digital finance, and global supply chains introduces new vulnerabilities. Cases like Huawei and Kaspersky Lab underscore persistent concerns about espionage and data security. Supply chain attacks by state-backed actors further reveal how weaknesses in business ecosystems can be exploited.

European Union initiatives, such as the Security Union Strategy, Digital Services Act, and the Chips Act, provide a multi-layered framework aimed at addressing these evolving threats. These policies stress collaboration across sectors, improved investment screening, and enhanced cybersecurity standards. National efforts, including Lithuania's strategic legislation and oversight mechanisms, reinforce this approach by protecting critical infrastructure, regulating foreign influence, and monitoring business activities in sensitive sectors.

To effectively mitigate these risks, a collaborative approach is essential—combining strong state regulation with responsible and transparent business practices. Regulatory bodies must ensure legal clarity, enforce compliance, and adapt to rapid technological change. As shown in the examples, in a digitalized and globalized world, national security starts with awareness—knowing service providers, their partners, and potential foreign connections. Enhancing legal frameworks and enforcing them consistently remains a necessary condition for safeguarding both economic interests and state security.

REFERENCES

[1] Republic of Lithuania, Seimas, "National Security Strategy," Resolution No. IX-907, May 28, 2002. [Online]. Available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.167925/asr. [Accessed: Mar. 3, 2025].

[2] Republic of Lithuania, Seimas, "Programme for the Strengthening and Development of the National Defence System," 2022. [Online]. Available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/e3acb430e78f11ee9fdedfc979ae62a9?jfwid=oizvypq8. [Accessed: Mar. 3, 2025].

[3] A. L. Friedberg, "The changing relationship between economics and national security," in *Power, Economics, and Security: The United States and Japan in Focus*. Routledge, 2019. [E-book]. Available: https://doi.org/10.4324/9780429302831.

[4] European Union, "Treaty on European Union" (Consolidated version 2016), Official Journal of the European Union, OJ C 202, Jun. 7, 2016.

[5] European Union, "Treaty on the Functioning of the European Union (Consolidated version 2016)", Official Journal of the European Union, OJ C 202, Jun. 7, 2016.

[6] European Union, Charter of Fundamental Rights of the European Union, Official Journal of the European Union, OJ C 364/01, Dec. 18, 2000.

[7] A. Banevičienė, "The regulation of non-horizontal concentrations in the context of EU economic security," in Transformations, Challenges and Security: Collective Monograph, Ž. Simanavičienė, Ed. Vilnius: Mykolas Romeris University, Public Security Academy, 2024. [Online]. Available: https://cris.mruni.eu/cris/handle/007/49074. [Accessed: Mar. 4, 2025].

[8] European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee, and the Committee of the Regions on the EU Security Union Strategy, COM(2020) 605 final, Jul. 24, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605. [Accessed: Mar. 4, 2025].

[9] European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee, and the Committee of the Regions: EU Agenda and Action Plan on Drugs 2021-2025, COM(2020) 606, Jul. 24, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0606. [Accessed: Mar. 4, 2025].

[10] European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee, and the Committee of the Regions: 2020-2025 EU Action Plan on Firearms Trafficking, COM/2020/608 final, Jul. 24, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0608. [Accessed: Mar. 4, 2025].

[11] European Commission, Communication from the Commission to the European Parliament and the Council on the Seventh Progress Report on the Implementation of the EU Security Union Strategy, COM(2024) 198 final, May 15, 2024. [Online]. Available: https://commission.europa.eu/publications/seventh-progress-report-implementation-eu-security-union-strategy_en. [Accessed: Mar. 4, 2025].

[12] European Parliament and Council, "Directive 2024/1260 (EU) of 24 April 2024 on Asset Recovery and Confiscation, Official Journal of the European Union", OJ L 2024/1260, May 2, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2024/1260/oj/eng. [Accessed: Mar. 4, 2025].

[13] European Commission, Proposal for a Directive of the European Parliament and of the Council on Combating Corruption, Replacing Council Framework Decision 2003/568/JHA and the Convention on the Fight Against Corruption Involving Officials of the European Communities or Officials of Member States of the European Union and Amending Directive (EU) 2017/1371 of the European Parliament and of the Council, COM/2023/234 final, May 3, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023PC0234. [Accessed: Mar. 4, 2025].

[14] European Parliament and Council, Directive 2022/2557 (EU) of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC, Official Journal of the European Union, OJ L 333, Dec. 27, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng. [Accessed: Mar. 4, 2025].

[15] European Parliament and Council, Directive 2022/2555 (EU) of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive), Official Journal of the European Union, OJ L 333, Dec. 27, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng. [Accessed: Mar. 4, 2025].

[16] European Commission, Proposal for a Council Recommendation on a Blueprint to Coordinate a Union-Level Response to Disruptions of Critical Infrastructure with Significant Cross-Border Relevance, COM/2023/526 final, Sep. 6, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-

content/EN/TXT/?uri=celex%3A52023DC0526. [Accessed: Mar. 4, 2025].

[17] European Parliament and Council, Regulation (EU) 2024/2747 of 9 October 2024 Establishing a Framework of Measures Related to an Internal Market Emergency and to the Resilience of the Internal Market and Amending Council Regulation (EC) No 2679/98 (Internal Market Emergency and Resilience Act), Official Journal of the European Union, OJ L 2747, Nov. 8, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/2747/oj/eng. [Accessed: Mar. 4, 2025].

[18] European Parliament and Council, Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act), Official Journal of the European Union, OJ L 151, Jun. 7, 2019. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881. [Accessed: Mar. 4, 2025].

[19] European Parliament and Council, Regulation (EU) 2022/2554 of 14 December 2022 on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, Official Journal of the European Union, OJ L 333, Dec. 27, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng. [Accessed: Mar. 4, 2025].

[20] European Parliament and Council, Regulation (EU) 2024/2847 of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), Official Journal of the European Union, OJ L 2847, Nov. 20, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng. [Accessed: Mar. 4, 2025].

[21] European Parliament and Council, Regulation (EU) 2025/38 of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act), Official Journal of the European Union, OJ L 38, Jan. 15, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2025/38/oj/eng. [Accessed: Mar. 4, 2025].

[22] European Commission, Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 Supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by Establishing a Network Code on Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, Official Journal of the European Union, OJ L 1366, May 24, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg_del/2024/1366/oj/eng. [Accessed: Mar. 4, 2025].

[23] European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee, and the Committee of the Regions: European Wind Power Action Plan, COM/2023/669 final, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023DC0669&qid=1702455143415. [Accessed: Mar. 4, 2025].

[24] R. Teixeira, O. Carmi, P. Gattinesi, and P. Hohenblum, *Water Security Plan Implementation Manual for Drinking Water Systems*, JRC Publications Repository, Jan. 11, 2022. [Online]. Available: https://publications.jrc.ec.europa.eu/repository/handle/JRC126684. [Accessed: Mar. 4, 2025].

[25] European Commission, Joint Communication to the European Parliament and the Council on the Update of the EU Maritime Security Strategy and its Action Plan: "An Enhanced EU Maritime Security Strategy for Evolving Maritime Threats", JOIN/2023/8 final, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023JC0008. [Accessed: Mar. 4, 2025].

[26] European Parliament and Council, Regulation (EU) 2024/1679 of 13 June 2024 on Union Guidelines for the Development of the Trans-European Transport Network, Amending Regulations (EU) 2021/1153 and (EU) No 913/2010 and Repealing Regulation (EU) No 1315/2013, Official Journal of the European Union, OJ L 1679, Jun. 28, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/1679/oj/eng. [Accessed: Mar. 4, 2025].

[27] European Commission, *Joint Communication to the European Parliament and the Council: European Union Space Strategy for Security and Defence*, JOIN(2023)9, Mar. 10, 2023. [Online]. Available: https://ec.europa.eu/transparency/documents-register/detail?ref=JOIN(2023)9&lang=en. [Accessed: Mar. 4, 2025].

[28] European Parliament and Council, Regulation (EU) 2023/1781 of 13 September 2023 Establishing a Framework of Measures for Strengthening Europe's Semiconductor Ecosystem and Amending Regulation (EU) 2021/694 (Chips Act), PE/28/2023/INIT, Official Journal of the European Union, OJ L 229, Sep. 18, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2023.229.01.0001.01.ENG. [Accessed: Mar. 4, 2025].

[29] European Parliament and Council, Regulation (EU) 2024/1252 of 11 April 2024 Establishing a Framework for Ensuring a Secure and Sustainable Supply of Critical Raw Materials and Amending Regulations (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1724, and (EU) 2019/1020, Official Journal of the European Union, OJ L 1252, May 3, 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1252&qid=1720020986785. [Accessed: Mar. 4, 2025].

[30] European Parliament and Council, Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), PE/24/2024/REV/1, Official Journal of the European Union, OJ L 1689, Jul. 12, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng. [Accessed: Mar. 4, 2025].

[31] European Commission, "Joint Communication to the European Parliament, the European Council, and the Council on "European Economic Security Strategy"," JOIN/2023/20 final, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023JC0020. [Accessed: Mar. 4, 2025].

[32] Council of the European Union, Regulation (EC) 139/2004 of 20 January 2004 on the Control of Concentrations Between Undertakings (the EC Merger Regulation), Official Journal of the European Union, OJ L 24, Jan. 29, 2004. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2004/139/oj/eng. [Accessed: Mar. 4, 2025].

[33] European Parliament and Council, Regulation (EU) 2022/2560 of 14 December 2022 on Foreign Subsidies Distorting the Internal Market, PE/46/2022/REV/1, Official Journal of the European Union, OJ L 330, Dec. 23, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/2560/oj/eng. [Accessed: Mar. 4, 2025].

[34] European Parliament and Council, Regulation (EU) 2022/1925 of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), PE/17/2022/REV/1, Official Journal of the European Union, OJ L 265, Oct. 12, 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32022R1925. [Accessed: Mar. 4, 2025].

[35] European Parliament and Council, Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), PE/30/2022/REV/1, Official Journal of the European Union, OJ L 277, Oct. 27, 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065. [Accessed: Mar. 4, 2025].

[36] European Parliament and Council, Regulation (EU) 2019/452 of 19 March 2019 Establishing a Framework for the Screening of Foreign Direct Investments into the Union, PE/72/2018/REV/1, Official Journal of the European Union, OJ L 79I, Mar. 21, 2019. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2019/452/oj/eng. [Accessed: Mar. 4, 2025].

[37] European Parliament and Council, Regulation (EU) 2021/821 of 20 May 2021 Setting up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit, and Transfer of Dual-Use Items, PE/54/2020/REV/2, Official Journal of the European Union, OJ L 206, Jun. 11, 2021. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0821. [Accessed: Mar. 4, 2025].

[38] European Parliament and Council, Regulation (EU) 2023/2675 of 22 November 2023 on the Protection of the Union and Its Member States from Economic Coercion by Third Countries, PE/34/2023/REV/1, Official Journal of the European Union, OJ L 2675, Dec. 7, 2023. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2023/2675/oj/eng. [Accessed: Mar. 4, 2025].

[39] Republic of Lithuania, Seimas, "Law on the Protection of Objects Important for Ensuring National Security," No. IX-1132, Oct. 10, 2002. [Online]. Available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.189498/asr. [Accessed: Mar. 3, 2025].

[40] Republic of Lithuania, State Security Department and Second Operational Services Department under the Ministry of National Defence, "National Threat Assessment", Feb. 15, 2024. [Online]. Available: https://www.vsd.lt/wp-content/uploads/2024/03/GR-2024-02-15-LT-1-1.pdf. [Accessed: Mar. 3, 2025].

[41] Lex Mundi, *Global Foreign Investment Restrictions Guide: Lithuania*, 2024. [Online]. Available: https://www.lexmundi.com/guides/lex-mundi-global-foreign-investment-restrictions-guide/jurisdictions/europe/lithuania. [Accessed: Mar. 3, 2025].

[42] Republic of Lithuania, Seimas, "Criminal Code of the Republic of Lithuania," No. VIII-1968, Sep. 26, 2000. [Online]. Available: https://e-

seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.111555. [Accessed: Mar. 3, 2025].

[43] Republic of Lithuania, Seimas, "Law on Lobbying Activities," No. VIII-1749, Jun. 27, 2000. [Online]. Available: http://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.104674/asr. [Accessed: Mar. 3, 2025].

[44] Chief Official Ethics Commission of the Republic of Lithuania, "Transparency Information System, 2025". [Online]. Available: https://skaidris.vtek.lt/public/home/main. [Accessed: Mar. 3, 2025].

[45] Republic of Lithuania, Seimas, "Law on Political Organizations," No. XIV-1450, Dec. 20, 2022. [Online]. Available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/a81b677034fa11edbf47f0036855e731. [Accessed: Mar. 3, 2025].

[46] Republic of Lithuania, Ministry of National Defence, "National Cybersecurity Report," 2023. [Online]. Available: https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2023.pdf. [Accessed: Mar. 3, 2025].

[47] Republic of Lithuania, National Cyber Security Centre, "Lietuvos ir Ukrainos atstovai sėkmingai baigė pirmą kartą surengtą pramoninių technologijų kibernetinio saugumo kursą," 2025. [Online]. Available: https://www.nksc.lt/naujienos/lietuvos_ir_ukrainos_atstovai_sekmingai_baige_pirm.html [Accessed: Mar. 3, 2025]

[48] T. Akimova, O. Akimov, Y. Mihus, *et al.*, "Improvement of the methodological approach to assessing the impact of public governance on ensuring the economic security of the state," ФКДПТП, 2021. [Online]. Available: ResearchGate www.researchgate.net [Accessed: Mar. 4, 2025]. http://dx.doi.org/10.18371/fcaptp.v4i35.221969

[49] V. Franchuk, Z. Zhyvko, and A. Kuzior, "The impact of criminal revenue legalization on economic security," Proceedings of the International Conference on Business, Accounting, Management, Banking, and Economics (BAMBEL-21), 2021. [Online]. Available: https://www.atlantis-press.com/proceedings/bambel-21/125960308. [Accessed: Mar. 4, 2025] 10.2991/aebmr.k.210826.013

[50] European Court of Human Rights, UAB Braitin v. Lithuania, Application No. 37944/19, Judgment of 6 February 2024. [Online]. Available: https://hudoc.echr.coe.int/?i=001-225221. [Accessed: Apr. 13, 2025].

[51] European Court of Human Rights, UAB Ambercore DC and UAB Arcus Novus v. Lithuania, Application No. 37943/19, Judgment of 6 February 2024. [Online]. Available: https://hudoc.echr.coe.int/?i=001-225220. [Accessed: Apr. 13, 2025].

[52] Constitutional Court of the Republic of Lithuania, Case No. 14/04, Conclusion on the compliance of the actions of the President of the Republic of Lithuania R. P., against whom impeachment proceedings have been initiated, with the Constitution of the Republic of Lithuania, 31 March 2004. [Online]. Available: https://lrkt.lt/en/court-acts/search/170/ta1263/content [Accessed: Apr. 13, 2025].

[53] Constitutional Court of the Republic of Lithuania, Case No. 40/03, Decision on the compliance of the Decree No. 40 of 11 April 2003 by the President of the Republic of Lithuania 'On the granting of citizenship of the Republic of Lithuania by way of exception', insofar as it provides that citizenship of the Republic of Lithuania by way of exception is granted to J. B., with the Constitution of the Republic of Lithuania and paragraph 1 of Article 16 of the Law on Citizenship of the Republic of Lithuania, 30 December 2003. [Online]. Available: https://lrkt.lt/en/court-acts/search/170/ta1245/content. [Accessed: Apr. 13, 2025].

[54] Lithuania, Regional Administrative Court, Administrative Case No. eI2-3776-1114/2024, 2 May 2024.

[55] Supreme Administrative Court of Lithuania, Administrative Case No. eA-393-520/2023, 8 November 2023

[56] Ministry of National Defence of the Republic of Lithuania, Press Release, "The Court heard the MoD legal team: complaint from a company that is not safe for Lithuania's national interest was dismissed," 8 December 2021. [Online]. Available: https://kam.lt/en/the-court-heard-the-mod-legal-team-complaint-from-a-company-that-is-not-safe-for-lithuanias-national-interest-was-dismissed/. [Accessed: Apr. 13, 2025].

[57] Lithuania, Vilnius Regional Administrative Court, Administrative Case No. I-4964-764/2016, 4 November 2016.

[58] Republic of Latvia, Latvian State Security Service, "Annual Report 2024". [Online]. Available: https://vdd.gov.lv/uploads/materials/40/en/annual-report-2024.pdf. [Accessed: Mar. 4, 2025].

[59] Republic of Estonia, Government Office, "Horisondiseire 2024". [Online]. Available: https://www.riigikantselei.ee/sites/default/files/documents/2024-06/Horisondiseire%202024_EN.pdf. [Accessed: Mar. 4, 2025].

[60] C. E. Wallace, Testimony before the Senate Judiciary Committee, "Dangerous Partners: Big Tech and Beijing," 116th Congress, Mar. 4, 2020. [Online]. Available: https://www.fbi.gov/news/testimony/dangerous-partners-big-tech-and-beijing. [Accessed: Mar. 4, 2025].

[61] Statista, "Which Countries Have Banned Huawei?", 2020. [Online]. Available: https://www.statista.com/chart/17528/countries-which-have-banned-huawei-products/. [Accessed: Mar. 4, 2025].

[62] Q. Bu, "Behind the Huawei sanction: national security, ideological prejudices or something else?" China International Strategy Review, 2024. [Online]. Available: https://link.springer.com/article/10.1365/s43439-024-00112-6. [Accessed: Mar. 4, 2025].

[63] Lietuvos Bankas, "Lietuvos bankas revoked UAB Foxpay licence due to serious and systematic breaches", 2024. [Online]. Available: https://www.lb.lt/en/news/lietuvos-bankas-revoked-uab-foxpay-licence-due-to-serious-and-systematic-breaches. [Accessed: Mar. 4, 2025].

[64] Fintechnews Baltic, "Fintech in Lithuania in 2024: Foxpay Collapses, Kevin Declares Bankruptcy, AML Compliance Remains a Challenge," Jan. 6, 2025. [Online]. Available: https://fintechbaltic.com/10118/fintechlithuania/fintech-in-lithuania-in-2024-foxpay-collapses-kevin-declares-bankruptcy-aml-compliance-remains-a-challenge/. [Accessed: Apr. 13, 2025].

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 341-348

Swarming Terrorist Attack as an Evolving Threat for the European Security

Svetoslav Yordanov
Research Center of Extremism and Terrorism
Rakovski National Defence College
Sofia, Bulgaria
yordanov_sv@yahoo.com

***Abstract*- This paper examines contemporary terrorism as a self-improving system that adapts to changes in the security environment. The article focuses on the study of the swarming attack as a terrorist tactic to achieve a strategic effect. The purpose of the publication is to analyse the nature of the complex coordinated terrorist attack and identify the factors that define it as an existing threat to European security. The main research methods include document study, systematic analysis and "case study". The conclusions related to the change in the tactical methods used by terrorists will contribute to the development of adequate countermeasures by the competent authorities.**

Keywords- Al Qaeda, counterterrorism, Islamic State – Khorasan Province, swarming terrorist attack.

I. INTRODUCTION

Contemporary terrorism can be discussed as a complex threat that manifests itself in a variety of forms that depend on the type and structure of the terrorist unit, the measures imposed to counter terrorism by the countries on whose territory the terrorist formations operate, the degree of acceptance of the achievements of scientific and technological progress by terrorists and their application in their own operational techniques and procedures, and last but not least, the changes in the security environment as a result of the political and economic confrontation of global and regional powers.

Terrorist activity can be carried out both by decentralized, independent and self-radicalized actors, as well as by sleeper terrorist cells that operate through centralized control and in coordination with a large "mother" terrorist organization.

Islamist terrorist groups such as Al-Qaeda and the Islamic State (IS)/Daesh, which have more than a decade of history and combat experience, continue to carry out active propaganda and take responsibility for terrorist acts committed in different parts of the world. These terrorist organizations develop their activities in a systematic manner with clearly outlined strategic goals to promote the fundamentalist version of Islam and the revival of the caliphate. Tactically, Al-Qaeda and Daesh are evolving, learning from their mistakes, adapting to the counteractions of the security and defence authorities, changing their methods of training, recruiting and deploying fighters in the Dar al-Harb (from the Arabic language "Territory of War" [1], i.e. countries hostile to Islam). Terrorist groups, like business organizations, strive for sustainable development and effective management of human capital [2].

Large terrorist organizations have the human, financial and logistical resources to plan, organize and carry out complex multilateral terrorist attacks or so-called "swarming attacks". In modern world history, the largest terrorist attack of this type was the attack by Al-Qaeda against the United States on September 11, 2001, and the last swarming attack on the territory of the European Union was the terrorist act of the Islamic State in Paris (France) in November 2015. The multilateral terrorist attacks of the Pakistani Lashkar-e-Taiba in Mumbai (India) in November 2008, of Hamas against Israel in October 2023, of the Islamic State – Khorasan Province in Derbent, Makhachkala and Sergokala (Republic of Dagestan, Russian Federation) in June 2024 also achieved a strategic effect.

Despite the exponential increase in the number of individual terrorist attacks in Europe carried out by self-radicalized individuals over the past five years, the threat of a large-scale terrorist attack carried out by well-trained terrorists under the direct operational management of an established jihadist organization has not passed, and the dynamics of the security environment are helping to transform it from a possibility to a probability. This requires an examination of both the nature of the

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8481
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

swarming attack as a terrorist tactic and the drivers that make it a current threat.

II. MATERIALS AND METHODS

The purpose of this publication is to study the nature of the swarming terrorist attack and to determine the factors that influence its formation as a real threat to the security of the European continent. *The main research tasks* include: defining the concept of a swarming terrorist attack; analysis of the organizational units that carry out complex multilateral terrorist attacks and the tactical methods they use; identifying changes in the security environment that favour the accomplishment of a swarming terrorist attack on the territory of Europe.

The object of the study is complex coordinated attacks as a terrorist tactic to achieve a strategic effect, and *the subject* of the study is the causes and paths for the emergence of the threat of a swarming terrorist attack for European security.

The research is limited to examining cases of swarming type terrorist attacks carried out only by individuals and formations that follow the ideology of global jihad.

The needs of this study were realized through the use of *general scientific methods* such as systematic analysis, synthesis, comparison, generalization, document study, and descriptive "case study".

Due to the fact that much of the information of research interest is classified, and often part of ongoing investigations, for the purposes of the report, information from open sources was used, which was assessed according to criteria for reliability, accuracy and completeness.

III. RESULTS AND DISCUSSION

A. Origin and general characteristics of swarming terrorist attack

Dispersal or swarming is a military tactic known since ancient times. In the 4th century BC, the Chinese military strategist and general Sun Bin, in his treatise The Art of War [3] (not to be confused with Sun Tzu's The Art of War), defined the advantages of the tactic of dispersing forces when conducting combat operations against a stronger enemy whose forces are concentrated, noting that strategic advantage can only be achieved through a surprise attack, both in time and place.

Historically, the discussed military tactic was used [4] during the Peloponnesian Wars, the Punic Wars, in the Middle Ages by the Bulgarians, Mongols, and Ottomans, and later even during World War II.

In its contemporary form, swarm tactics are used in maritime piracy raids in the Gulf of Aden [5], in carrying out complex coordinated terrorist attacks, as well as for rapid force projection in counterinsurgency and counterterrorism operations by security and defence forces.

The term "swarming" is also used to describe the use of multiple unmanned aerial vehicles [6] that work in a coordinated manner within a single control system to perform tasks for both military and civilian purposes.

The theoretical explanation of swarming attacks involves extrapolating animal behavioural patterns for the purposes of military tactics. In their daily activities for subsistence and defence, various animal species organize themselves into collective structural units that allow them to survive more easily in changing natural conditions and in collisions with hostile representatives of the human and animal kingdoms. According to research by the RAND think tank [7] on network warfare and the development of future armed conflicts, the relationship between nature and swarming attacks can be attributed as follows: the organizational behaviour of bees and ants to the tactics of guerrilla groups; the hunting of the wolf pack to the hooliganism of football fans; the behavioural pattern of flies and mosquitoes to the looting of marauders; the lifestyle of viruses and bacteria to the actions of street criminal gangs.

In the context under consideration, the use of swarming attacks by terrorist groups can be attributed to the behaviour of the wolf pack. Despite its limitations, such an analogy helps to deduce and understand the main distinguishing features of the terrorist tactics under study. Similarities are observed in terms of numbers, deliberate aggressiveness, hierarchical dependence, preferred selection of soft targets, opportunism, and reliance on the element of surprise.

In the context of warfare, swarming attacks seek a tactical advantage, as the enemy's security and defence system is overcome asymmetrically, deliberately overloaded through rapid saturation of forces and resources across multiple diverse targets, which leads to a high level of uncertainty, a low degree of predictability, and an increase in response time in the event of a crisis.

A distinctive feature of terrorism is that it uses indiscriminate projection of force, relying on various unconventional tactics and techniques that allow it to achieve high political, economic, social and psychological impact. The synergistic approach multiplies the effect of individual forms and methods [8], and the characteristics of the swarming attack determine it as suitable for implementation by extremist and terrorist groups, which is also facilitated by the development of high technologies.

In essence, a swarming terrorist attack is a complex, multilateral, coordinated terrorist attack in which separate groups of terrorists attack a single target from several directions or different targets, simultaneously or in a short period of time. The location of the attack objects can be in the same administrative-territorial unit, as well as in neighbouring or nearby ones, using a variety of tactical techniques.

In counterterrorism theory, there is no consensus definition of a complex coordinated terrorist attack, but several definitions can nevertheless be distinguished.

According to the United States Cybersecurity and Infrastructure Security Agency (CISA) operational manual, a complex coordinated terrorist attack is *"a violent attack or series of attacks by one or more individuals or groups using one or more types of weapons with the intent to cause harm to a large number of people"* [9].

Some weaknesses are noted in the definition presented in this way. The emphasis is placed on the quantitative indicator of perpetrators, human casualties, attacks and types of weapons, without mentioning the heterogeneity of the targets in terms of type, direction of attack, location and time, as well as the connecting element of synchronization and coherence.

According to the United States Department of Homeland Security, complex coordinated terrorist attacks are *"acts of terrorism that are carried out by synchronized and independent teams at multiple locations in succession or close succession, initiated with little or no warning, and using one or more weapons systems such as firearms, explosives, arson, and other unconventional attack methods, which are intended to result in a large number of casualties"* [10]. It is noteworthy that this definition develops a previous one cited in a scholarly publication, namely that a complex coordinated terrorist attack is *"a coordinated attack at one or more locations in close succession, initiated with little or no warning, using one or more of the following: firearms, explosives, and arson"* [11].

In the two definitions above, the authors focus on the temporal factor, the minimal possibility of advance notice of the attack, the specific means of attack, the multiplicity of targets, the coherence of the actions of the individual attacking groups and the loss of human lives. In general, the second definition could be expanded, especially since the tactical methods are limited, which places a restriction on the weapons used and does not reflect the objective reality in its entirety. The characterization proposed by Homeland Security does not allow some of the coordinated attacking terrorist structures to be composed of only one person, but emphasizes "synchronized and independent teams", without making it clear whether these groups of terrorists are independent in terms of a single operational command or independently carry out the attack against each specific target.

The following characteristics relevant to the swarming terrorist attack can be identified:

- Hybridity – expressed in the combined use of various tactical techniques such as automatic firearms, simple and complex improvised explosive devices (including those mounted on unmanned aerial vehicles), edged weapons, vehicle attacks, etc.
- Suddenness – expressed in the rapid deployment of forces without prior indication of their intentions to attack
- Asymmetry – expressed in attacking "soft" enemy targets
- Autonomy – projected in the independent logistical support of the fighters and the selection of the tactical method
- High mobility – expressed in the ability to attack targets situated in a location other than the permanent residence of the terrorists and the leadership of the terrorist organization, as well as in the ability for a quick planned withdrawal after the attack
- Uncertainty – expressed in terms of manifestation in time and space, which leads to low predictability
- Flexibility – expressed in the ability of terrorists to adapt to the security measures of the competent authorities and change the choice of their targets
- High intensity – projected to saturate forces and resources against enemy targets in a short time
- Complexity – expressed in the high level of planning and organization, maintaining a high level of combat readiness by terrorists, as well as the ability to attack targets in different domains such as land, air, water and cyberspace
- Coordination – projected in the coordinated attack against multiple targets by different terrorist groups or attacking one key target by many sides
- Strategic effect – as a result of the terrorist attack, a long-term qualitative change is achieved in the political, economic and social system of the enemy

Based on the analysis, the following definition of a swarming terrorist attack can be proposed:

A swarming terrorist attack is a pre-planned, coordinated multi-vector terrorist attack, in which several separate terrorist units attack with different tactical methods simultaneously or in a short temporal interval multiple heterogeneous targets or one target from several sides, aiming for the maximum number of human casualties and large material damage.

The structure of the proposed definition includes:

- *The essential features of the concept* – a pre-planned coordinated multi-vector terrorist attack
- *The subjects of the terrorist attack* – separate terrorist units (a unit is understood as a small organizational unit)
- *The objects of the terrorist attack* – multiple heterogeneous targets or one target from several countries
- *The specific manner of carrying out the attack* – using different tactical techniques
- *Time frame* – simultaneously or in a short temporal interval

- *The desired effect of the attack* – maximum number of human casualties and large material damage

B. Case study

There are several emblematic "swarming" terrorist attacks carried out due to Islamist motives on the territory of the European continent in the last ten years - the terrorist attacks in Paris (France) in November 2015, the bombings in Brussels (Belgium) in March 2016, the attack in London (Great Britain) in June 2017 and the terrorist act in Moscow (Russia) in March 2024.

The cases are selected based on the criteria - relevance, multilateralism and complexity of the attack, diversity of targets and tactical approaches, and a large number of dead and wounded.

Although the above-mentioned events have been studied many times, for the purposes of this research, they should be analysed comprehensively in their entirety and interconnectedness. Indicators of scientific interest include: profile of the perpetrators; nature of the targets; affiliation with a large terrorist organization; tactical methods used; number of dead and injured.

TABLE 1 MAIN ATTRIBUTES OF THE SWARMING TERRORIST ATTACKS IN EUROPE

Location and date	Attackers	Targets	Tactical methods	Deaths	Injured
Paris, 2015	9	6	2	130	350
Brussels, 2016	5	2	1	32	340
London, 2017	3	1	2	8	48
Moscow, 2024	4	1	3	145	500

The terrorist attack in Paris, carried out on the evening of November 13, 2015, is the largest terrorist act in the recent history of France and an event that changed the security environment throughout Europe.

The attack was carried out by ten terrorists (9 direct perpetrators, including the terrorist group's leader, as well as one logistician who was supposed to blow himself up at the first target, but gave up), divided into three teams, who attacked 6 targets at three different locations. The total number of deaths from all targets of the terrorist attack is 130, and the number of injured is 350, with the highest number of victims (90) at the last location (in shooting at the concert hall) [12].

The first group of terrorists blew themselves up at two of the entrances to the French national stadium in the suburb of Saint-Denis and next to a restaurant in the area of the sports facility, using vests with improvised explosive devices (so-called "martyr belts"). These terrorists failed to complete their mission due to their failure to enter the audience, in which only one person died besides themselves and about fifty were injured.

The second squad used indiscriminate street shooting against visitors to various cafes, bars and restaurants in two administrative districts close to each other (the 10th and 11th), with one of the attackers blowing himself up.

The third team attacked the Bataclan concert hall, with the terrorists firing randomly with automatic weapons, and in the subsequent contact with a police patrol that responded to the scene, one of the attackers blew himself up. The remaining two jihadists take hostages, after which the Special Forces storm the building. The terrorists are eliminated, with one of them, although wounded managing to activate the explosive device he was carrying.

The Brussels bombings were carried out by five terrorists, divided into two teams, consisting of three and two fighters respectively, who attacked two targets – the capital's airport and a train leaving a metro station near the Council of the European Union and the European Commission headquarters. 32 people were killed and another 340 were injured [13].

The first team of three suicide bombers attacked Brussels Airport, with two terrorists detonating two improvised explosive devices in suitcases in the departure area within a few seconds. The third terrorist hesitated and escaped without carrying out his mission.

The second team of two terrorists was scheduled to detonate improvised explosive devices in backpacks they were carrying in the capital's metro trains. Only one jihadist succeeded, while the other gave up and returned to his safe house.

Based on the analysis of publicly available information [14], the following profile of the fifteen terrorists who carried out the terrorist attacks in Paris and Brussels can be outlined: all between the ages of 20 and 31; second-generation immigrants with a predominant Moroccan origin and Belgian residence; combat experience gained as Daesh fighters in Syria; have a criminal past related to theft, fraud, forgery, possession and trafficking of narcotics, or have already come under the attention of the security services due to involvement in terrorist activity.

It is striking that a large part of the perpetrators have known each other well since childhood (having grown up in the Muslim neighbourhoods of Brussels) and have participated in different types of crimes together. Sharing common fates and long-standing friendships help build trust, which is realized in group radicalization and in successful teamwork in the preparation and execution of terrorist acts.

Some of the jihadists also have family ties - two of the perpetrators of the attacks in Paris are brothers, as are two of the suicide bombers in Brussels. This once again proves the role of the family environment in the radicalization process and emphasizes that when individual members of a family unit follow a common

radical ideology, this can develop into a form of family terrorism [15].

Regarding the terrorist cell's management system and the planning, preparation, organization, and execution of the discussed terrorist acts in Paris and Brussels, a three-tier chain of command can be outlined: a field officer who is directly responsible for carrying out terrorist attacks on a territorial basis and directs them on the ground; a tactical-level commander who prepares, organizes, coordinates, and directs the attacks from a remote command and control center in Belgium; and a unified operational command of the Islamic State that plans all terrorist operations in Western Europe.

The terrorist cell also shows signs of network decentralization and autonomy in making tactical decisions, as well as flexibility and adaptability in the event of loss of strength and the emergence of extraordinary circumstances. When the terrorist, who is a tactical-level commander, is eliminated in a clash with the Belgian security authorities [16], the group tasked with carrying out the bombings against the airport and the metro in Brussels continues to act according to plan and a week later carries out the two coordinated attacks. It can be concluded that in terms of decision-making autonomy, the terrorist operation resembles a special military operation in urban conditions, when in conditions of information deficit and uncertainty, the initiative of field commanders [17] is essential for the successful implementation of the assigned tasks. At the same time, the management of the terrorist cell also uses "integrative processes to synchronize various specific functions" [18].

In terms of coordination and timing of the terrorist acts in Paris and Brussels, the Daesh cell showed exceptional precision in its planning. The attacks on the three different locations in Paris began at 21:20, 21:25 and 21:40 [19], respectively, and the bombings of the airport and the metro in Brussels at 07:58 and 09:11 [20]. The purpose was to create a shock effect on the security systems of the attacked countries, which led to a lack of reaction time and a concentration of forces and resources by law enforcement agencies at all the attacked locations, overloading emergency telephone lines, hospitals and the fire department, and blocking public transport. In France, the terrorist operation was controlled in real time by the field commander, as well as by the remote command and control center in Brussels, which was in constant communication with the terrorist teams.

On the evening of 3 June 2017 [21], three individuals of Moroccan and Pakistani origin carried out a terrorist attack in London, driving a van into pedestrians on the pavement of London Bridge. After their vehicle crashed, the terrorists got out and began stabbing indiscriminately at people walking along the streets to nearby bars. The attack left 8 dead and 48 injured [22], and the Islamic State claimed responsibility for the attack. Interestingly, the jihadists used ceramic kitchen knives, which are easily accessible and can pass through metal detectors without hindrance. The attackers were aged between 22 and 30, were self-radicalised and showed visible signs of praising radical Islam and terrorism, and two of them had come under the attention of the security services, with one even being a member of the UK-designated terrorist group Al-Muhajiroun [23]. No direct operational leadership of the attack by the Islamic State has been established.

On the evening of 22 March 2024 [24], four individuals of Tajik origin carried out a coordinated terrorist attack on the Crocus City Hall concert hall in Moscow, firing indiscriminately with automatic weapons, stabbing the wounded, and starting a fire with improvised incendiary devices, killing 145 people and injuring over 500. The Islamic State Khorasan Province claimed responsibility for the attack, with the terrorist organization publishing a photo of its fighters [25] making the "jihad" sign and posing against a Daesh flag. The attack was carried out with exceptional audacity, being well-planned and prepared, despite the high security measures in Russia.

TABLE 2 ASSESSMENT OF THE SWARMING TERRORIST ATTACKS IN EUROPE

Location and date	Intensity	Complexity	Effect
Paris, 2015	High	High	High
Brussels, 2016	Medium	High	High
London, 2017	High	Low	Medium
Moscow, 2024	High	Medium	High

The four terrorist attacks studied (Paris, Brussels, London and Moscow) have all the characteristics of a swarming terrorist attack, which allows them to be compared in terms of intensity, complexity and achieved effect, and to highlight some differences.

The attack in France is of high intensity, high complexity and high effect. This is determined by the scale of the terrorist attack (6 targets in three different locations), the high level of organization, the diverse tactical methods and the short temporal interval for which the force was projected, as well as the large number of victims and injured.

The terrorist act in Belgium is of medium intensity, high complexity and high effect. Here the assessment of medium intensity is dictated by the larger interval during which the attacks at the airport and in the metro begin – about one hour, as well as the smaller number of attackers involved. The complexity comes from the coordination of an attack against two objects of critical infrastructure, which are strictly guarded. The effect remains high, despite the lower number of victims compared to Paris, as the attacks were carried out in a city where a number of European and international

institutions located (headquarters of the EU, NATO and the UN).

The attack in the UK is of high intensity, low complexity and medium effect. The high intensity is imposed by the short time in which the terrorist act was carried out (about 10 minutes), including contact with law enforcement agencies. The complexity is low, as easily accessible tactical means are used - vehicles and kitchen knives, and there is also no need to overcome complex protection systems. The effect is medium due to the small number of victims and injured, compared to the other cases considered, but still the publicity of the terrorist act and the attack on an emblematic architectural landmark in London achieve a sufficient effect.

The terrorist attack in Russia is of high intensity, medium complexity and high effect. High intensity is defined by the use of three tactical approaches in the attack on a large-scale facility, requiring only about 10 minutes for the execution of the mission and then quickly withdraw. Although it requires detailed planning, the terrorist act can be classified as medium complexity, since only one facility with a low level of security is attacked. High impact refers to the huge number of dead and injured, as well as to the large material damage.

C. Current drivers of the threat

The current drivers of the threat of new swarming terrorist attacks on the territory of Europe are developing in "a complex context of politics, security, international relations, law and sovereignty" [26], and they can be classified into several main groups related to the development of processes in the external and internal security environment.

The drivers that relate to the external security environment include:

- *The presence of key vital points that are a haven for global jihadism.* These are countries or geographical areas in which, for political reasons, terrorists can develop their recruitment, training and financing activities in conditions of relative freedom and even cooperation with local authorities. Currently, such areas are located in Afghanistan, Yemen, Somalia, Mali, Burkina Faso, Niger, Congo, etc.
- *Regional conflicts that have a global projection in terms of the radicalization process*. The unresolved Israeli-Palestinian conflict contributes to the encapsulation of religious and ethnic foundations in Europe and the accumulation of sentiments for the violent resolution of ideological disputes.
- *Activity of large and established terrorist groups such as Al-Qaeda and the Islamic State.* These terrorist organizations continue to carry out active propaganda in their media outlets such as Amaq, Al-Azaim, Thabat, Al-Naba, distribute practical manuals for violent jihad, have significant financial resources, and take responsibility for terrorist attacks.
- *Increase in illegal migration*. Conflict zones create conditions for the movement of large masses of people and the infiltration of extremists and terrorists into illegal migrant flows, including those with combat experience and plans for future terrorist attacks on the territory of Europe.
- *Illicit trafficking in small arms and light weapons*. The war in Ukraine contributes to the presence of a large number of small arms and light weapons in circulation, which is exploited by organized crime, which illegally imports them into Europe and can sell them to various radicalized individuals ready to commit a terrorist act.
- *Globalization of high technology and information connectivity*. The widespread use of cryptocurrency trading helps diversify the sources and methods of financing terrorism, and the development of mobile applications for anonymous and encrypted communication facilitates the communication security of terrorists and terrorist organizations.

Drivers related to the internal security environment include:

- *Lowering the age limit for radicalization in Europe*. The steady trend of increasing numbers of minors and juveniles arrested in Europe for involvement in terrorist activities creates a prerequisite for their easier recruitment by large terrorist organizations and their involvement in the preparation and execution of a complex coordinated terrorist attack.
- *Loss of intelligence positions*. It is related to the redirection and commitment of intelligence resources to other areas, such as the war in Ukraine, as well as to the decisions to withdraw forces and assets from various hot spots in Africa (France from Mali, Burkina Faso and Niger) and Afghanistan (termination of missions to support international peace and security).
- *Defects in legislation and the criminal process*. Weaknesses in the national legislation of some countries hinder the effective criminal prosecution of persons accused of terrorist activities.
- *Unidentified returned foreign fighters*. A large part of European citizens who fought on the side of various extremist and terrorist groups in Africa and the Middle East, including in the ranks of the Islamic State, remain off the radar, with some of them not falling into the established risk profiles, and others having entered European territory among the flows of illegal migrants, using false identity documents.

- *Increasing vulnerability to radicalization of marginalized social groups*. The formation of peculiar ghettos in large European cities leads to encapsulation, rejection of secular education, non-recognition of the authority of state institutions and easy acceptance of radical models of behaviour and communication with those who are different.
- *Increasing street crime.* Practical cases show that a large proportion of perpetrators of terrorist acts in Europe have criminal records for involvement in petty crimes, which helps to blur the line between good and evil, legal and illegal, and makes it easier to involve them in terrorist activity.

IV. Conclusions

It can be concluded that the more time passes since the last complex and coordinated terrorist act on the territory of Europe, the more the probability of a new one increases. Planning, preparing and organizing a large swarming attack require intelligence, logistical and financial support in the conditions of conspiratoriality and network decentralization. The improvement of the system for countering terrorism in European countries leads to a search for new forms and methods for organizing large terrorist attacks by terrorist groups.

It can be predicted that, trying to overcome state security systems, terrorist organizations will evolve mainly in terms of the profile of the fighters who are assigned to participate in complex coordinated attacks, their level of training, as well as the tactical methods used.

It is possible that the new profile of the terrorist will be characterized by a pure criminal past, hidden signs of radicalization, good social status and integration into European societies, as well as the use of more and more women and children in attacks. The possible revival of dormant terrorist cells will increase the level of unpredictability and enhance the effect of surprise.

At the tactical level, it is possible to use drones with installed improvised explosive or incendiary devices, as the costs of making them are not high, and some of the terrorists already have similar combat experience in Syria. The other threat is related to the use of poisons, chemical and biological weapons, as access to precursors is facilitated by weak border control in Afghanistan and Syria, and scientists and experts can be attracted, both on a voluntary basis and through threats.

Effective counteraction to the organization and conduct of swarming terrorist attacks requires the acquisition of information in advance by creating intelligence sources among the commanders of terrorist organizations, individuals and entities that support terrorism, and among opposition resistance movements, as well as the use of know-how operational combinations.

References

[1] "Dar al-Harb", in The Oxford Dictionary of Islam. Oxford University Press. [Online]. Available: Oxford Reference, https://www.oxfordreference.com/display/10.1093/oi/authority.20110803095700308. [Accessed: February 1, 2025].

[2] V. Vasilev, D. Stefanova and C. Popescu, "Human Capital Management and Digitalization – From Good Practices and Traditions to Sustainable Development", Digitalization, Sustainable Development, and Industry 5.0, B. Akkaya, S. A. Apostu, E. Hysa and M. Panait, Ed. Leeds: Emerald Publishing Limited, 2023, pp. 41-65. [Online]. Available: ResearchGate, https://www.researchgate.net/publication/375767230_Human_Capital_Management_and_Digitalization_-_From_Good_Practices_and_Traditions_to_Sustainable_Development. [Accessed: February 21, 2025]. https://doi.org/10.1108/978-1-83753-190-520231004.

[3] D. C. Lau and R. T. Ames, Sun Bin: The Art of Warfare: A Translation of the Classic Chinese Work of Philosophy and Strategy. New York: State University of New York Press, 2003.

[4] S. J. A. Edwards, „Swarming on the Battlefield: Past, Present, and Future". CA: RAND Corporation, 2000. [Online]. Available: RAND, https://www.rand.org/pubs/monograph_reports/MR1100.html. [Accessed: February 2, 2025].

[5] N. Childs, „Navies struggle with 'swarming' pirates", BBC News, April 1, 2010. [Online]. Available: http://news.bbc.co.uk/2/hi/africa/8598726.stm. [Accessed: February 2, 2025].

[6] A. Alotaibi, C. Chatwin, and P. Birch, "A Secure Communication Framework for Drone Swarms in Autonomous Surveillance Operations", "Journal of Computer and Communications", vol. 12, no. 11, p. 1-25, November 2024. [Online]. Available: SCIRP, https://www.scirp.org/journal/paperinformation?paperid=137084. [Accessed: February 2, 2025], https://doi.org/10.4236/jcc.2024.1211001

[7] P. Marinov, "Processes of Radicalization and Development of Terrorist Activity", "Defence Against Terrorism Review – DATR", vol. 15, pp. 35-54, June 2022. [Online]. Available: ResearchGate, https://www.researchgate.net/publication/361170285_Defence_Against_Terrorism_Review_-_DATR_Processes_of_Radicalization_and_Development_of_Terrorist_Activity. [Accessed: February 3, 2025].

[8] J. Arquilla and D. Ronfeldt, „Swarming and the Future of Conflict". CA: RAND Corporation, 2000. [Online]. Available: RAND, https://www.rand.org/pubs/documented_briefings/DB311.html. [Accessed: February 3, 2025].

[9] Cybersecurity and Infrastructure Security Agency, "Complex Coordinated Attacks Action Guide", Cybersecurity and Infrastructure Security Agency, September 2019. [Online]. Available: https://www.cisa.gov/resources-tools/resources/complex-coordinated-attacks-action-guide. [Accessed: February 3, 2025].

[10] U.S. Department of Homeland Security, "Planning Considerations: Complex Coordinated Terrorist Attacks", Homeland Security, July 2018. [Online]. Available: FEMA, https://www.fema.gov/sites/default/files/2020-07/planning-considerations-complex-coordinated-terrorist-attacks.pdf. [Accessed: February 3, 2025].

[11] T. Elliott, "Complex Coordinated Terrorist Attack: Considerations for Practical Emergency Preparedness and Resiliency Exercises". Dayton, Ohio: Wright State University, 2017. [Online]. Available: CORE Scholar, https://corescholar.libraries.wright.edu/cgi/viewcontent.cgi?article=1200&context=mph. [Accessed: February 3, 2025].

[12] Q. Williams, "The Attacks on Paris: Lessons learned". Los Angeles: Homeland Security Advisory Council, June 2016.

[Online]. Available: Pepperdine University, https://publicpolicy.pepperdine.edu/hsac/content/hsac-paris-lessons-learned_whitepaper.pdf. [Accessed: February 10, 2025].

[13] France 24, "Ten suspects to face trial in deadly 2016 Brussels bombings case", January 5, 2021. [Online]. Available: https://www.france24.com/en/europe/20210105-ten-suspects-to-face-trial-in-deadly-2016-brussels-bombings-case. [Accessed: February 10, 2025].

[14] P. Cruickshank, "The inside story of the Paris and Brussels attacks", CNN, October 30, 2017. [Online]. Available: https://edition.cnn.com/2016/03/30/europe/inside-paris-brussels-terror-attacks/index.html. [Accessed: February 10, 2025].

[15] D. Ivanov, "THE NUCLEAR FAMILY IN MODERN TERRORISM", ETR, vol. 4, pp. 121–124, Jun. 2024, https://doi.org/10.17770/etr2024vol4.8220.

[16] BBC News, "Paris and Brussels bombers' links uncovered", April 9, 2016. [Online]. Available: https://www.bbc.com/news/world-europe-35879401. [Accessed: February 12, 2025].

[17] C. V. Nistorescu, "Key Milestones in Urban Operations", BULLETIN OF "CAROL I" NATIONAL DEFENCE UNIVERSITY, vol. 13, no. 4, pp. 7–22, 2025, https://doi.org/10.53477/2284-9378-24-45.

[18] G.-I. Toroi, "Rethinking military command and control systems", BULLETIN OF "CAROL I" NATIONAL DEFENCE UNIVERSITY, vol. 13, no. 4, pp. 88–112, 2025, https://doi.org/10.53477/2284-9378-24-51.

[19] J. Maloney and D. Morgan, "The Paris Terrorist Attacks – Implications for first responders", Journal of High Threat & Austere Medicine, vol. 1, no. 1, pp. 1-8, July 2019, [Online]. Available: Cambridge Media, https://journals.cambridgemedia.com.au/application/files/6016/8359/7173/Maloney_Paris_2019.pdf. [Accessed: February 15, 2025].

[20] S. Clarke, P. Torpey, C. Levett, G. Swann, P. Allen, F. Sheehy and S. Jeffery, "Timeline of the Brussels attacks", The Guardian, March 22, 2016. [Online]. Available: https://www.theguardian.com/world/ng-interactive/2016/mar/22/where-the-brussels-attackers-struck. [Accessed: February 15, 2025].

[21] BBC News, "London Bridge attack: What happened", May 3, 2019. [Online]. Available: https://www.bbc.com/news/uk-england-london-40147164. [Accessed: February 20, 2025].

[22] J. Kleeman, "They were killed in the London Bridge terror attack, seconds apart. So why did their families get wildly different payouts?", The Guardian, March 9, 2024. [Online]. Available: https://www.theguardian.com/uk-news/2024/mar/09/london-bridge-terror-attack-why-did-victims-families-get-wildly-different-payouts. [Accessed: February 20, 2025].

[23] D. Anderson, "Attacks in London and Manchester between March and June 2017", Home Office, July 2018, ISBN: 978-1-78655-598-4. [Online]. Available: GOV UK, https://www.gov.uk/government/publications/attacks-in-london-and-manchester-between-march-and-june-2017. [Accessed: February 3, 2025].

[24] BBC News, "What we know about attack on a Moscow concert hall", April 9, 2024. [Online]. Available: https://www.bbc.com/news/world-europe-68645755. [Accessed: February 21, 2025].

[25] S. Yan, "Islamic State attackers publish selfie following Moscow attack", The Telegraph, March 23, 2024. [Online]. Available: https://www.telegraph.co.uk/world-news/2024/03/23/why-did-isis-k-attack-a-moscow-theatre/. [Accessed: February 21, 2025].

[26] R. Marinov, "CONTEMPORARY CHALLENGES TO THE PROTECTION OF THE COUNTRY'S SOVEREIGNTY",*ETR*, vol. 4, pp. 168–172, Jun. 2024, https://doi.org/10.17770/etr2024vol4.8187.

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025.Volume V, 349-352

Methodology For Assessment of A National Security System

Zarko Zdravkov
The Defense Advanced Research Institute (DARI)
National Defense College "G. S. Rakovski"
Sofia, Bulgaria
z.zdravkov@rndc.bg

Anelia Atipova
The Defense Advanced Research Institute (DARI)
National Defense College "G. S. Rakovski"
Sofia, Bulgaria
a.atipova@rndc.bg

***Abstract*— The nature of modern threats poses serious challenges to national security systems. They are forced to undergo transformations with high intensity and structural impact in order to adapt to the security environment. The iterative nature of the problem and the constantly changing context of its updating necessitate the study of the structural and functional integrity of national security systems. The report presents a methodology for assessing a proposed model of a national security system, in the sense of a set of management bodies and their functions. To achieve the goal, generally accepted methods of analysis were used: system analysis (structural, functional), analysis and synthesis, induction and deduction, mathematical modeling, criterial analysis and risk analysis methods. The results obtained are a summary of independently conducted expert assessments of the proposed model, based on criteria that represent the objective state of the system. They include recommendations for improving: the attainability of the goals, the adequacy of the structure and functions of the model.**

Keywords—national security system; strategic assessment; evaluation methodology; formal model; governing bodies.

I. INTRODUCTION

The dynamic nature of modern threats and the deficiencies in the structure and activities of institutions of national security systems require their continuous improvement and achievement of the necessary maturity level, to adapt to the requirements of the environment.

This methodology offers a comprehensive and systematized approach to the assessment of a proposed model of a national security system, based on its in-depth study, through the application of proven, modern methods of analysis.

To achieve the scientific goal of the methodology, an analysis of the environment of the functioning of a national security system is carried out. On this basis, the system is assessed and proposals for improvement in the proposed model are formulated.

The methodology is applicable to the assessment of a model of a national security system at a strategic level.

II. MATERIALS AND METHODS

The methodology defines the purpose, scope and necessary tools of the study. It is carried out by applying: system analysis (structural, functional), analysis and synthesis, induction and deduction, mathematical modeling, criterial analysis and risk analysis methods.

Open sources materials have been used to conduct the analysis.

The final result of the analysis is a summary of assessments of experts, applying the methodology independently of each other.

III. RESULTS AND DISCUSSION

A. Environment For the Creation of a National Security System

The creation of a national security system is carried out in the context of the real environment of the functioning of the state, which forms the general conditions for the implementation of state policies in the field. Therefore, its adequacy is determined not only by the approach to construction, the completeness and connectivity between the components, but also by the environment of functioning.

a) National security system operating environment

The operating environment of a national security system is determined by national legislation, adopted union commitments and bilateral agreements. The institutions of the national security system, as such, perform their functions in the field of security and defense policy,

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8480
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

through the development of strategic, conceptual, program and planning documents, the adoption of regulatory acts, the introduction of standards, the performance of observations, the preparation of analyses and other activities specific to the respective field.

B. National Security System Assessment

The national security system consists of state bodies and structures that carry out the following types of activities: diplomatic, defense, intelligence, counterintelligence, operational-search, law enforcement and security activities [1]. Their functioning is supervised by a collective body (Council or Secretariat) with consultative and coordination functions.

a) Formal model of a national security system

For the analysis of a national security system, a Formal Model is created and criteria for evaluating its components are introduced.

The formal model of a national security system provides a description of the components of the system appropriate to the needs of the methodology and sets the framework within which the analysis is carried out.

The model describes the relationship between the bodies of a national security system and the functions for ensuring security at the national (strategic) level.

Definition 1: National Security System Formal Model (NSSFM) is called the sequentially ordered 3 components:

$$NSSFM_i = \{G_k, F_m, O_n\},$$

where: i is the relation number of a function to a governing body;

G_k - goal, k is the sequential number of the goal, $G_k \in K$, K is a multiplicity of goals;

F_m – governance function, m is the sequential number of the function, $F_n \in M$, M is a multiplicity of governance functions;

O_n – governing body, n is the sequential number of the body, $O_n \in N$, N K is a multiplicity of governing bodies.

b) Goal

The goal is "a specific desired achievement, state or reaction". The goals are defined in the adopted national strategic documents and are included in the regulatory framework. They are achieved by the body through its assigned functions.

c) Functions

The function is "a specific, relatively distinct area of the organization's or structural unit's activity, involving the performance of interrelated operations" [2]. Each function should be considered as a set of activities. When an activity is part of more than one function, this activity should be distinguished as an independent function.

The functions are identified within the areas of activity imposed by the requirements for the security environment and are linked to the goal. A function can be performed by one or more bodies.

The protection of national security requires actions in 4 areas (Table 1):

1. Analysis of the specifics and dependencies in the security environment and early warning of the occurrence of risks.
2. Prevention, reduction and prevention of risks.
3. Crisis management and response.
4. Identification, designation and protection of critical infrastructure.

The identified functions are filled in as shown in Table 1.

TABLE 1 FUNCTIONS OF GOVERNING BODIES

Directions	**Function**		
	Governing Body 1	***.....***	***Governing Body N***
Direction 1	*Function*	.....	*Function*
	.....	.....	.....
	Function	.....	*Function*
Direction 2	*Function*	.....	*Function*
	.....	.....	.....
	Function	.....	*Function*
Direction 3	*Function*	.....	*Function*
	.....	.....	.....
	Function	.....	*Function*
Direction 4	*Function*	.....	*Function*
	.....	.....	.....
	Function	.....	*Function*

d) Governing Bodies

Governing bodies are the Head of State, the legislative body and the executive bodies. These are state structures formed according to the law with power powers granted to them in connection with the tasks they perform [3]. They are in certain relationships of dependence with other bodies.

In addition to being the object of analysis, state bodies are bearers of functions in the subject area and beneficiaries of goal setting and control [4].

Executive bodies are divided into hierarchical groups (Table 2):

1. Governing bodies of administrative structures reporting their activities to the legislative body.
2. Central executive bodies.
3. Governing bodies of specialized territorial administrations established as legal entities by an administrative act.
4. Territorial executive bodies.

The formal model of a national security system covers bodies and structures from all groups.

The identified bodies are filled in Table 2.

TABLE 2 DEFINING MULTIPLE BODIES IN GROUPS

Groups	*Bodies with governing, coordination and control authorization*		
Group 1	*Governing body*	.....	*Governing body*
Group 2	*Governing body*	.....	*Governing body*
Group 3	*Governing body*	.....	*Governing body*
Group 4	*Governing body*	.....	*Governing body*

The description of the organs as a component of the formal model provides their basic characteristics on the basis of which they can be evaluated.

The tabular representation of the formal model is shown in Table 3.

TABLE 3 TABULAR REPRESENTATION OF THE FORMAL MODEL OF THE NSS

№	**Function**	**Governing body**
1	**2**	**3**
1.	***Goal***	
1.1.	*Function*	*Governing body*
1.2.	*Function*	*Governing body*
.....	.....	.....
N	*Function*	*Governing body*
2.	***Цел***	
2.1.	*Function*	*Governing body*
2.2.	*Function*	*Governing body*
.....	.....	.....
N	*Function*	*Governing body*

C. Assessment of the National Security System Model

The assessment of the national security system is carried out separately for each of the components of its formal model, according to established criteria.

The criteria for assessing the components of the national security system model are as follows:

a) Criteria for assessing functions

The functions identified in column No. 2 of Table 3 are assessed against the goal to which they relate, according to the following criteria:

1. Criteria for achieving a goal:

- Criterion 1.1. "Availability for achievement" – assesses the availability of functions for achieving the specified goal.
- Criterion 1.2 "Relevance" – assesses the relationship of the functions to the goals of the institutions and structures of the National Security System.

The functions identified in column No. 2 of Table 3 are assessed against the bodies to which they relate, according to the following criteria:

b) Criteria for distribution by bodies:

- Criterion 2.1. "Distribution" – assesses the distribution of functions between the bodies to achieve the goal.
- Criterion 2.2. "Contradiction" – assesses the contradiction of the functions of the bodies to achieve the goal.
- Criterion 2.3. "Duplication" – assesses the duplication of the functions of the bodies to achieve the goal.

c) Criteria for assessing the bodies

The identified bodies in column No. 3 of Table 3 are assessed against the goal to which they relate, according to the following criteria:

- Criterion 2.1. "Purpose" – indicates the presence of goals of the bodies, their type and connectivity. The information it provides serves for a subsequent assessment of the relevance of the functions to the bodies.
- Criterion 2.2. "Subordination" – assesses the hierarchical arrangement of the bodies in the formal model of the SZNS to achieve the goal.
- Criterion 2.3. "Coordination" – assesses the existence and type of mechanisms for coordinating actions to achieve the goal between the bodies of the formal model of the NSS.

D. Recommendations for updating the current NSS model

In view of its improved functioning, the following groups of recommendations should be made:

a) Achievability of the goal/s

1. Recommendations on the availability of functions in relation to the goals
2. Recommendations on the relevance of functions in relation to the goals

b) Adequacy of the structure

3. Recommendations on the availability of functions in relation to the bodies
4. Recommendations on the subordination of management bodies
5. Recommendations on the coordination of management bodies.

c) Combination of functions

6. Recommendations on the contradiction of functions in relation to the bodies
7. Recommendations on the duplication of functions in relation to the bodies.

d) Additional recommendations

Recommendations for correcting discovered shortcomings in information processing that are beyond the scope of the criteria in the methodology (for example, terminological correctness, etc.) are allowed.

E. Reporting the results

The methodology involves the performance of uniform independent expert assessments, which are combined into a report. As a final assessment of each aspect, the overcoming hypotheses in the expert assessments are summarized. It is compiled in the Bottom Line Up Format format [5] and contains the following components:

- Key points (a synthesized presentation of the main points in the text, a summary of the supporting points in the analysis);
- Introduction (contains: the basis for performing the assessment, a brief description of the researched document, the purpose of the study, the method of conducting the study (methodology, number of expert assessments), presentation of the experts participating in the study and the team performing the summary in the final report);
- Exposition (follows the analysis according to the steps in the methodology);
- Conclusion (includes: the conclusions, a summary of the content of the document, presents an expanded reading of existing ideas in the text, without introducing new ones; contains a predictive element);
- References;
- Appendices (forms from the methodology to be completed in the suggested sequence).

IV. CONCLUSIONS

The methodology offers an approach for assessing a formal model of a national security system, according to established criteria. The parameters of the model are goals of the strategic management process, existing bodies and their functions - management, monitoring and control. They are assessed according to criteria affecting their structure and functionality.

The model claims to be universal and highly applicable, because it proceeds from the general principles of strategic management and represents individual units in the sense of their functions, taking into account the variable nature of their hierarchical location in the system and subordination restrictions.

For the objectivity of the analysis, the model is considered in conditions of real functioning of the state. The recommendations made allow for corrective actions with regard to the purpose, structure and functions of the bodies, in view of their sufficiency, complementarity and degree of coordination.

The methodology is applied by independent specialists with expertise in individual subject areas. The results obtained are summarized and systematized in an expert assessment of the model of a national security system.

The methodology was tested in a report on the topic "Assessment of the National Security Protection System in the Republic of Bulgaria", presented at the International Scientific Conference of the G. S. Rakovski Military Academy on the topic "20 Years of Bulgaria in NATO and NATO in Bulgaria" [6].

V. ACKNOWLEDGMENTS

The Methodology for evaluating strategic documents was created in implementation of the National Scientific Program "Security and Defense", Component 3 "Defense and Protection of the Population in Disasters and Accidents", Work Package 3.2 "Doctrines and Strategies", Work Task, 3.2.1. “Exploring Security Concepts, Doctrines, and Strategies. Modeling the National Security System”.

VI. REFERENCES

[1] Law on the Management and Functioning of the National Security Protection System of the Republic of Bulgaria, Lex.bg - Закони, правилници, конституция, кодекси, държавен вестник, правилници по прилагане [Accessed Oct. 9, 2024].

[2] Unified methodology for conducting functional analysis in state administration, 2019, p. 5, (Портал за обществени консултации) (strategy.bg) [Accessed Oct. 10, 2024].

[3] Integrated Information System of the State Administration, (Органи на изпълнителната власт)(government.bg) [Accessed October 13, 2024].

[4] Law on Administration, Promulgated in the State Gazette, No. 130 of 5 November 1998, Art. 19, Lex.bg (Закони, правилници, конституция, кодекси, държавен вестник, правилници по прилагане)[Accessed October 16, 2024].

[5] BLUF: The Military Standard That Can Make Your Writing More Powerful, https://www.animalz.co/blog/bottom-line-up-front/ [Accessed October 15, 2024].

[6] A. Atipova, "Assessment of the National Security Protection System in the Republic of Bulgaria", Military Journal, issue 2s / 2024, pp. 30-44, ISSN 0861-7392

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 353-361

Key Takeaways from the Most Significant GDPR Personal Data Breaches in the Republic of Bulgaria

Martin Zahariev
Faculty of Information Sciences, National Security Department
University of Library Studies and Information Technologies
Sofia, Bulgaria
m.zahariev@unibit.bg

George Dimitrov
Faculty of Information Sciences, Computer Sciences Department
University of Library Studies and Information Technologies
Sofia, Bulgaria
g.g.dimitrov@unibit.bg

Daniela Pavlova
Faculty of Information Sciences, Computer Sciences Department
University of Library Studies and Information Technologies
Sofia, Bulgaria
d.pavlova@unibit.bg

Panayot Gindev
Information Systems and Technologies Department
University of Library Studies and Information Technologies
Sofia, Bulgaria
p.gindev@unibit.bg

Vyara Savova
University of Library Studies and Information Technologies
Sofia, Bulgaria
vyara.savova@yahoo.com

Radoslava Makshutova
Institute for the State and the Law
Bulgarian Academy of Sciences
Sofia, Bulgaria
r.makshutova@gmail.com

***Abstract*—The present research paper focuses on the most significant personal data breaches under the EU General Data Protection Regulation 2016/679 (GDPR) that took place in the Republic of Bulgaria since the GDPR became applicable in 2018. These include *inter alia* the data breaches that affected the National Revenue Agency, the Bulgarian Posts, one of the Bulgarian banks and other organizations from the public and the private sector. The analysis of these cases is important, because they had an impact on thousands and sometimes millions of people and resulted in severe sanctions reaching thousands and sometimes millions of Bulgarian leva. This problem is especially relevant in the modern information society where the collection and processing of data are fundamental for the economic growth and societal well-being. By examining the available public documentary sources on these cases such as the practice of the Bulgarian Commission for Personal Data Protection Commission the authors aim to derive key takeaways regarding the reasons for these data breaches, the gaps in the data protection and information security practices of the affected organizations and possibly to synthesize recommendations and advice for the future how such breaches could be avoided or at least mitigated. These results will play a valuable part in a broader scientific research project dedicated to management of the data breach response reaction processes of the Bulgarian organizations funded by the Bulgarian Science Fund with the Ministry of Education where the authors form the research team.**

***Keywords*— Bulgarian organizations, data breach, GDPR, gaps.**

I. INTRODUCTION

The present study aims to explore the most significant personal data breach cases that affected organizations from the public and private sector in the Republic of Bulgaria – a Member State of the EU. The goal of this analysis is to find the main reasons that led to the said data breaches and to systematize key takeaways from these unfortunate events. Ultimately, the present paper argues that the data breach cases subject to the research are caused by a variety of factors and that their understanding and addressing is an important precondition so that in future such breaches could be prevented or at least, the severity of the consequences arising out of them could be limited.

The background of this research lies in the EU the General Data Protection Regulation 2016/679 (the Regulation/GDPR) [1] that was adopted with the idea to enhance the protection of the individuals in the context of the drastically increased data processing activities in the era of digital transformation and to foster the scrutiny of the organizations that collect and process personal data by

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8482
© 2025 The Author(s). Published by RTU PRESS.
This is an open access article under the Creative Commons Attribution 4.0 International License.

envisaging new data obligations for the controllers and processors, by expanding existing ones and by providing for broader data subjects' rights. Among other things, GDPR introduced reporting obligations in case of data breaches towards the supervisory authority (Article 33) and in certain cases – towards the affected individuals (Article 34). The doctrine explains that as follows: *"This obligation shall protect the rights and freedoms of the data subject by way of a better level of transparency."* [2]. The data breach reporting *"through notifications and communications is essentially a transparency requirement that shines the spotlight on operational failure and the resulting risks"* [3]. This new obligation enabled the society in general to find out about significant data breaches that affected various organizations which ultimately made the present research possible.

II. Materials and methods

The results of the present study were obtained after applying scientific methods such as:

Documentary method – consisting in analyzing and synthesizing information about the legal regime for GDPR data breach reporting and from various documentary sources – e.g. from the secondary EU law, from Bulgarian national legislation, from the practice of the Bulgarian data protection authority and from other publicly available (including online) sources, as well as in the systematization and summarization of this information.

Deductive and inductive reasoning – these methods are used with regard to the deriving of certain conclusions/scientific observations from the specific cases to the general and *vice versa*.

Comparative analysis – this method consists of comparing the common and the different between separate phenomena. In this report, this method is used to highlight some common reasons and mistakes that led to the occurrence of data breaches.

Case study – this method is used for analyzing real cases in order to collect new knowledge regarding the reasons for occurrence of data breaches and the measures to mitigate such breaches.

III. Results and discussion

Among the most notable cases are the data breaches that impacted the National Revenue Agency, Bulgarian Posts and one of the leading private banks in the country. These breaches resulted in the exposure of personal data, including special categories of data, affecting millions or hundreds of thousands of individuals and prompting investigations and sanctions by the Bulgarian Commission for Personal Data Protection (CPDP). This section provides an overview of these incidents, highlighting their impact and the following regulatory response.

A. The Data Breach in the Bulgarian National Revenue Agency

In August 2019 the CPDP imposed the biggest fine under GDPR in Bulgaria to the National Revenue Agency (NRA) for infringement of Article 32, para. 1, lit. b) of the Regulation [4]. Along with the fine, the CPDP issued an order to the NRA to undertake appropriate technical and organizational measures [5] (on the basis of Article 58, para. 2, lit. d) in conjunction with Article 57, par. 1, lit. a) and Article 83, para. 2, lit. a), c), d), f) and g) of the Regulation).

The data breach was a result of a cyberattack on the NRA's systems. Databases of around 11 gigabytes were sent anonymously to different Bulgarian media outlets, as well as made public online, and after further investigation it was confirmed that they contained personal data of more than 5 million persons from the NRA's systems (later the number was confirmed to be 4 104 786 active Bulgarian and foreign citizens). The prosecutor's office initiated criminal proceedings against two persons (one of the proceedings is ongoing as of 14 February 2025) [6]. The CPDP started an investigation upon notification of the data breach it received from the NRA on 17 July 2019. Following the investigation, numerous individuals initiated court proceedings for compensation for the infringement of their rights under the Regulation. One of the damage claim proceedings [7] led to a preliminary request to the Court of Justice of the European Union (CJEU) on which it issued a ruling interpreting the Regulation. In addition, collective claim proceedings were initiated.

a) Penalty Order and Fine

On 28.08.2019 the CPDP issued a penalty order to the NRA and imposed a fine of BGN 5 100 000 (approx. EUR 2 607 500) for failure to comply with the requirements of Article 32, para.1, lit. b) of GDPR. The order itself is not public, but according to CPDP's bulletin [8] the penalty was based on unauthorized access, unauthorized disclosure and dissemination of personal data of individuals from the information databases maintained by the NRA. The penalty order was confirmed by the first level court in subsequent proceedings, then revoked by the second level court, and then again revoked due to expiry of the statute of limitations. The first level court stipulated that on the factual and legal side the acts described in the penalty order were indisputably established and that the sanction imposed was correctly determined [9]. The second level court revoked the first level court's decision due to the expiry of the statute of limitations without discussing the case in essence [10].

Key takeaway: these proceedings did not lead to any final conclusion on whether NRA complied with its obligation to apply appropriate technical and organisational measures.

b) Decision for Adoption of Appropriate Technical and Organisational Measures

On 22.08.2019 the CPDP issued a decision [5] enlisting twenty data protection measures to be adopted by the NRA. They included: to establish clear rules, responsibilities, and interaction procedures for different system users; to improve the security of personal data in e-service applications; to develop comprehensive data protection

policies for all the NRA information systems; to ensure restrictive access policies to databases; to introduce audit logs and systems for managing privileged access and security event analysis; to develop a risk management methodology, including threat identification and periodic risk assessments; to conduct risk analysis and establish operational rules for data processing systems; to perform impact assessments for systems identified as high-risk; to set procedures for data protection impact assessments when launching new systems; to adapt information systems to the GDPR requirements, including risk management procedures for new or modified systems; to upgrade outdated operating systems and database management systems to mitigate security risks; to establish a disaster recovery center for real-time system recovery; to define policies for processing of special categories of data; to create policies for handling children's data; to develop encryption strategies for archived and one-time query data; to update the job description and responsibilities of the Data Protection Officer, ensuring direct reporting to the executive director; to revise employee job descriptions to include data processing responsibilities; to establish internal training programs for the NRA employees on handling personal data breaches.

The decision was later revoked partially by the first level court [11]. During the court proceedings the NRA presented information and documents on its data protection measures prior and following the data breach and appealed the decision on numerous grounds, including short deadlines for completion, general and unclear wording, incorrect findings and conclusions of the inspection team. The court repealed the decision in the parts concerning measures imposed by the CPDP. In respect to the performance of a risk analysis of systems and processing operations the court pointed out that risk analysis was performed on a regular basis in accordance with a procedure established by the executive director of the NRA. Regarding the requirements to establish policies for the re-use of subjects' personal data, including children's data, the court stipulated that the Regulation and the Bulgarian data protection legislation lack legal norms regulating the necessity and grounds for the creation of special rights for the re-use of personal data. In addition the court found that the NRA had developed rules for archiving data and the court did not find a need to explicitly introduce additional anonymisation, archiving and destruction rules for electronic data used on a one-time basis. Finally the court found that actions to establish audit records of the individual events and logs for privileged usershad already been implemented.

However, this decision was partially repealed by the second level court [12] due to procedural infringements of the first level court and the case was returned to the first level for re-examination (as of 14 February 2024 no final decision has been issued).

Key takeaway: no final decision on whether the NRA applied appropriate technical and organisational measures, however, the second level court adopted partially the arguments of the NRA against the measures imposed by the CPDP.

c) Claims for Damages by Individuals

Following the data breach, numerous affected persons filed claims for compensation for damages caused by the NRA as data controller. While some of the claims were successful before the first level court, the second level court mainly stipulated that "*the mere fact of unauthorized access to the NRA's information system does not prove the defendant's failure to protect it"*. This view was later confirmed by the CJEU in a preliminary ruling (see lit. e) below). The court also based its decision on its lack of expertise on the matter: "*since the court does not have special knowledge to assess what was done, whether what was done was sufficient, whether the hacker attack could have been avoided and if yes, what else should have been done, the court should have (….) ex officio admitted the hearing of forensic technical expertise on this issue*" [13]. In other words, in most of the proceedings the second level court stipulated that the first level court did not carry out the necessary procedural actions to assess whether there was wrongdoing on behalf of the NRA. As a result, it returned the proceedings to the first level court for re-examination. The re-examination led to varying end results. After forensic technical expertises were carried out, it was established that the NRA had developed various adequate rules and policies concerning network and information security, but they were not effectively implemented in practice. Given this, the court found that there was unlawful inaction on the part of the NRA in fulfilling the obligations arising from the relevant legal provisions to ensure the reliability and security of its information system. As a controller, the NRA was required to take effective measures to prevent malicious access to personal data, including crimes, and it failed to do so. However, the court did not rule in favor of the claimants in all cases, as in some cases it stipulated that there was no proof of damages (for example no proof of leakage of personal data of the particular claimant). Other proceedings were terminated due to expiry of the statute of limitations or on procedural grounds. The compensations, where granted, were in small amounts up to BGN 500 (EUR 255).

Key takeaway: varying final decisions, but generally the re-examination of the cases led to confirmation of unlawful inaction by the NRA and granting of compensations, albeit in small amounts.

d) Collective Claims

In addition to the individual claims, there have been collective claims aimed at forcing the state to take appropriate measures for personal data protection in the NRA's systems. The proceedings on one of these collective claims started in November 2024 and it is expected that the court will allow claimants to join until March 2025 [14], while others have already been terminated due to procedural reasons [15].

Key takeaway: it is to be seen whether the current proceedings will lead to imposition of further obligations for personal data protection on the NRA.

e) Preliminary Ruling of the CJEU

One of the individual claims against the NRA led to the decision of the Supreme Administrative Court to request a preliminary ruling of the CJEU [16]. All court proceedings related to the data breach were suspended until the CJEU issued its ruling and the re-examination decisions of the first level court described above were issued after the proceedings were renewed (there may be exceptions). In the ruling, the CJEU stipulated that unauthorised disclosure of personal data or unauthorised access to those data by a 'third party' are not sufficient, in themselves, for it to be held that the technical and organisational measures implemented by the controller in question were not 'appropriate'. The appropriateness of the measures must be assessed by the national courts in a concrete manner, by taking into account the risks associated with the processing concerned and by assessing whether the nature, content and implementation of those measures are appropriate to those risks. In addition, the CJEU stipulated that the principle of accountability must be interpreted as meaning that, in an action for damages the controller bears the burden of proving that the security measures implemented by it are appropriate. In order to assess the appropriateness of the security measures an expert's report cannot constitute a systematically necessary and sufficient means of proof. The controller cannot be exempt from its obligation to pay compensation for the damage suffered by a data subject solely because that damage is a result of unauthorised disclosure of, or access to, personal data by a third party in which case that controller must then prove that it is in no way responsible for the event. The fear experienced by a data subject with regard to a possible misuse of his or her personal data by third parties as a result of an infringement of that regulation is capable, in itself, of constituting 'non-material damage' within the meaning of the Regulation.

Key takeaway: due to the NRA data breach proceedings the CJEU cleared out in what cases controllers shall compensate individuals in case of unauthorised disclosure to a third party and how the application of appropriate technical and organizational measures shall be assessed.

The NRA data breach happened undoubtedly due to lack of cybersecurity measures capable of stopping a particular attack on the systems. However, there is no definitive answer on whether the NRA failed to apply 'suitable' measures and on whether it infringed the GDPR. There is also no definitive decision on what measures the NRA applied successfully, what measures it failed to apply prior to the data breach, and what measures it must start applying in the future. The judicial proceedings following the NRA breach indicated that the Bulgarian court system was not prepared to apply data protection legislation to a case of such a scale. This led to multiple procedural conundrums, contradicting conclusions, delays and even expiry of the statute of limitations.

d) The Bulgarian National Revenue Agency Data Breach – Recommendations for Improvement

The case provides several key takeaways in different directions. First, the case demonstrates the necessity of independent oversight and stricter accountability mechanisms for public institutions handling significant quantities of personal data. While for some controllers the risk of intentional attacks is lower, the NRA data breach clearly demonstrates that public institutions in Bulgaria must be extra aware of malicious and intentional actions against their systems, and to apply proactive approach. The case outlines the necessity for public institutions to constantly keep up to date with most recent developments in technologies and data protection, or else it may be hard to argue that they took appropriate protection measures. From another point of view, the case demosntrates the supervisory's approach to high-impact matters, which may need improvement in the future – as numerous of the objections of the supervised institution NRA were upheld in court. Lastly, the examined data breach sheds a light on the approach of courts to such matters. As a key takeaway from the judicial proceedings, each data breach resulting from external actions must be carefully and thoroughly examined, including by technical experts. Courts must not stipulate that an attacked entity did not apply appropriate measures solely because the attack was successful; however, any conclusion that the attacked entity is not at fault solely because the data breach was caused by external intentional actions must also be considered ill-grounded.

Hopefully, the accumulated case law and the ruling of the CJEU will aid judges in similar cases in the future in Bulgaria and other EU Member States.

B. The Bulgarian Posts and a Leading Bulgarian Bank Data Breaches

In April 2022, the national postal service provider, Bulgarian Posts, suffered a severe cyberattack that disrupted its operations and compromised the personal data of 675,393 people whose identification was made possible through the affected personal data. The attack, reportedly a ransomware incident, led to system outages, preventing the processing of financial transactions, pension payments, and mail deliveries for an extended period of time. The breach exposed customers' personal data, including personal identification numbers and addresses, as well as information about financial transactions and people's health status.

Investigations indicated that the attack exploited vulnerabilities in Bulgarian Posts' outdated IT infrastructure. Due to insufficient cybersecurity measures and a lack of proper incident response strategies, the attackers managed to paralyse critical services, highlighting the weaknesses in the National Post's security framework. The attack was identified as being carried out using the Mimikatz malware, a credential theft tool, allowing unauthorised access to administrative accounts. Hackers infiltrated the SQL cluster containing personal

data, encrypted large portions of databases, and even encrypted backup files, rendering data recovery practically impossible [17].

The compromised information included personal identification numbers, addresses, financial data, pension details, and even medical records indicating the level of a person's disability. In total, approximately 4.67 million records were affected. The attack leveraged a security vulnerability in the Post's not-up-to-date Microsoft email server, enabling the hackers to gain full access to the virtual infrastructure and encrypt the backup data storage [18].

a) Regulatory and Institutional Response to the Bulgarian Post's Data Breach

The CPDP, as the regulatory body responsible for overseeing data protection in the country, launched an immediate investigation into the breach, focusing on compliance with the GDPR and the applicable national data protection laws. The findings revealed serious deficiencies in the organisation's cybersecurity preparedness, including outdated software, insufficient monitoring, a lack of timely risk assessments regarding the Post's backup and log file policies, and a low level of password management among the personnel. These impaired Bulgarian Post's ability to ensure continued confidentiality, availability, integrity, and resilience of the data processing systems and services and promptly restore availability and access to personal data.

As a result, the CPDP determined that Bulgarian Posts had failed to implement appropriate technical and organisational measures, violating specific articles of the GDPR. These include Article 32, para. 1, lit. b), c), and d), which outline the security measures that data controllers must implement to protect personal data, and para. 2, in connection with Article 5, para. 1, lit. e) of the GDPR, which requires data controllers to ensure the security and integrity of personal data. Furthermore, the CPDP deemed it most appropriate to apply the measure under Article 58, para. 2, lit. d) of the GDPR, namely, to issue specific instructions to the controller, including guidance on how to rectify the identified violations, and a sanction in the among of BGN 1,000,000 (approximately EUR 511,000). The CPDP's Administrative Sanctions Decision (Decision No. PAIKD-13-20/22 of 06.10.2022, issued by the Commission for Personal Data Protection was later challenged in court by Bulgarian Posts but upheld by the Administrative Court of Sofia as lawful. [17], [18].

In 2019, a major private bank in Bulgaria suffered a severe data breach affecting approximately 33,500 customers. The breach involved unauthorised access to 23,270 credit dossiers containing personal data, including special categories of data and financial information. Unlike the Bulgarian Posts case, which resulted from an external cyberattack, the private bank breach was due to internal security failures, particularly in data handling practices during an outsourced document digitisation process [19].

The CPDP investigation following the data breach determined that the bank, as a data controller, failed to implement suitable technical and organisational measures to protect the confidentiality, integrity, availability, and resilience of personal data processing systems.

The breach resulted in unauthorised access to a broad range of personal data, including names, national identification numbers, citizenship status, and addresses; copies of personal identification documents, including biometric data; tax documents detailing income and health insurance status; medical data, including official medical disability decisions; bank account numbers and transaction records; notarial deed registration numbers and signatures [19].

The investigation revealed that the breach stemmed from inadequate security measures during a large-scale credit dossier digitisation project, which took place between 2014 and 2016. The bank had outsourced the process but failed to enforce proper oversight and secure the deletion of scanned records, leaving sensitive information accessible on the scanning devices. This subsequently led to unauthorised third parties obtaining copies of credit dossiers.

b) The Bulgarian Post's Data Breach – Recommendations for Improvement

The cyberattack on the Bulgarian Posts highlighted severe deficiencies in cybersecurity preparedness, particularly in the organisation's outdated IT infrastructure, lack of proper monitoring, and ineffective incident response strategies. To prevent similar incidents in the future, it is essential to adopt a comprehensive cybersecurity strategy that includes regular software updates, security patching, and continuous penetration testing to identify and mitigate vulnerabilities before they can be exploited. Strengthening access control measures through the implementation of a suitable security model would significantly reduce the risk of unauthorised access. This approach ensures that all users, whether internal or external, are continuously verified and granted only the minimum necessary access to perform their tasks.

Furthermore, the attack was particularly damaging because the hackers managed to encrypt backup files, rendering data recovery nearly impossible. To address this risk, Bulgarian Posts and other public institutions should implement a multi-layered backup strategy that includes offline backups and immutable storage solutions. These measures would ensure that, even in the event of a ransomware attack, data recovery remains possible. Additionally, given that inadequate password management and poor security awareness among employees contributed to the breach, the introduction of mandatory cybersecurity training programs should be a priority. Regular training on phishing threats, secure password management, and incident response protocols would significantly enhance the organisation's ability to prevent and contain future attacks.

To prevent similar incidents in the postal sector, the implementation of sector-specific cybersecurity strategies is essential. *Admass et al.* recommend not only technical protections like encryption and intrusion detection but also

fostering collaborative cybersecurity ecosystems across public institutions to ensure readiness and rapid response to threats [20].

c) Regulatory and Institutional Response to the Private Bank's Data Breach

The CPDP concluded that the private bank violated Article 32 of GDPR, failing to ensure adequate data protection measures. Key security lapses included a lack of encryption for scanned documents, inadequate access controls and oversight over the scanning process and a failure to delete customer data from scanning devices after the digitisation project ended.

As a result, the CPDP imposed a fine of BGN 1,000,000 BGN (approximately EUR 511,000) on the private bank for unlawfully exposing the personal data of 33,492 clients, as well as an unknown number of third-party individuals linked to them, such as spouses, sellers, legal heirs, and guarantors.

The bank appealed the fine, arguing that it had followed industry-standard security practices and that liability should be shared with the external contractor. However, after multiple court reviews, the Administrative Court of Sofia City upheld the penalty, affirming that the bank bore ultimate responsibility as the data controller [21].

Key takeaway: due to the Bulgarian Posts and the private bank data breach proceedings, the CPDP clarified the obligations of both public institutions and financial entities in implementing technical and organizational measures to prevent unauthorized access, emphasizing, among other things, the importance of secure data management, encryption, and oversight in outsourced processes to ensure GDPR compliance.

d) The Private Bank Data Breach – Recommendations for Improvement

The data breach at one of Bulgaria's leading private banks revealed critical weaknesses in the oversight of third-party service providers, as well as in the bank's internal data security practices. Given that the breach stemmed from an outsourced document digitisation process, financial institutions must enforce strict contractual obligations for external service providers, ensuring that all third parties handling sensitive data comply with internationally recognised security standards, such as ISO 27001 or NIST cybersecurity frameworks. Regular audits and security assessments should be required to verify that these providers implement and maintain appropriate technical and organisational measures.

To further mitigate risks associated with outsourcing and third-party access to sensitive personal data, banks must implement robust master data management (MDM) systems and data governance frameworks. As *Martins et al.* argue, compliance with international standards like BCBS 239 requires banks to develop centralised, well-documented data architectures with clearly assigned ownership and lifecycle controls, supported by board-level governance structures and internal audits [22] (The "BCBS 239" concept refers to the "Principles for Effective Risk Data Aggregation and Risk Reporting" by the Bank of International Settlement. made publicly available by the Basel Committee on Banking Supervision in early 2013. From a structural perspective, BCBS 239 is organised around a set of 14 Principles that draw attention to the diverse obligations and concerns that must be addressed when managing risk in banking institutions [22]). This approach could not only enhance compliance, but also enables risk-based decision-making and transparency across all data domains.

Additionally, the bank's failure to securely delete scanned documents after the completion of the digitisation process demonstrates the need for strict data retention and deletion policies. Automated data lifecycle management should be implemented to ensure that unnecessary data is permanently removed once it is no longer required for business or regulatory purposes.

The slow response to the breach further underscores the necessity of a well-defined and regularly tested incident response plan. Banks and other financial institutions should conduct periodic cybersecurity drills and tabletop exercises to ensure that their teams can respond swiftly and effectively to potential data breaches. Strengthening these security measures would not only improve compliance with GDPR but also reinforce public trust in the banking sector's ability to safeguard sensitive personal and financial information.

C. Other Significant Data Breach Cases in Bulgaria

After analyzing the cases related to the massive data breach at the NRA, as well as the incidents at Bulgarian Posts and one of the Bulgarian banks, it becomes clear that insufficient security measures and risk management remain a serious problem in both the public and private sectors. In addition to these examples, a few more notorious data breach case seem relevant for the purposes of the present analysis.

a) The Data Breach in the Supreme Administrative Court

Bulgaria recently witnessed another major incident related to the security of judicial institutions. A hacker attack affected the Supreme Administrative Court (SAC) and all administrative courts in the country, leading to a temporary disruption of the Unified Administrative Court Case Management System and raising questions about the level of cybersecurity in the judicial system [23].

Subsequently, it became clear that the hacker group Ransomhouse took responsibility for the attack by posting a message on the Dark Web and stating that they had copies of data from the SAC. To support their claims, the hackers released part of the compromised information, including personal data of judicial employees, which according to specialized sources was already accessible to hundreds of users on illegal platforms.

This attack differs from traditional ransomware attacks because instead of encrypting files, Ransomhouse uses an

extortion model based on threats of public distribution of the stolen data. An additional concern is that the attack was carried out using one of the most sophisticated malware, White Rabbit, which is believed to have penetrated the system due to human error. This not only reveals vulnerabilities in the cybersecurity of judicial institutions but also underscores the lack of effective protocols for prevention and response to such incidents. Although the SAC received emergency funding to improve its infrastructure, the attack raises serious questions about the overall resilience of state information systems against organized cybercrime groups.

This attack is further evidence of the increasing risks to data protection in the public sector and highlights the need for stricter preventive measures, including better control over access to critical systems, regular training to recognize phishing attacks, and strategic investments in cyber resilience. Considering the cases already analyzed, attention should also be paid to other significant breaches that differ in nature but nonetheless reveal similar weaknesses in the approach to personal data protection. In this context, the next two cases focus on the Inspectorate to the Supreme Judicial Council (ISJC) and a violation related to the unauthorized publication of sensitive personal data, as well as on a case of lapses in information access management in the educational and accounting sectors [24].

b) The Data Breaches in the Inspectorate to the Supreme Judicial Council and in the Areas of Education and Accounting

In July 2019, the ISJC in its capacity as a personal data controller published in its electronic register 4420 declarations of assets and interests for 2018 of judges, prosecutors, and investigators. In some of these declarations (pertaining to 20 judges, prosecutors, and investigators and the related 19 spouses and 11 minors), personal data were disclosed that were not minimized, including personal identification numbers, ID card numbers, addresses, telephone numbers, and social information. This represents a violation of Article 5, para. 1, lit. e) and Article 32, para. 1, lit. b) and c) of the GDPR, as well as Article 66, para. 1 of the Bulgarian Personal Data Protection Act [25].

The main reason for the incident appears to be a combination of inadequate organizational measures to protect personal data and a lack of automated mechanisms to minimize sensitive information before its publication. There may have been insufficient control over the process of anonymizing personal data, leading to their unintentional disclosure. Also, the publication of such a volume of information in such a short period suggests that there may have been pressure to fulfill administrative obligations without sufficient technological and expert resources for verification. The ISJC was imposed an administrative penalty of 2000 BGN (approximately EUR 1000), according to Article 87, para. 3 of the Bulgarian Personal Data Protection Act. Although this penalty may seem insignificant, it underscores the need for improving control mechanisms in public institutions.

The second case involves two private schools and an accounting firm, which reported a personal data breach to the CPDP under Article 33 of the GDPR. During the investigation, it was found that the schools had provided access to their information system to the accounting firm without ensuring appropriate technical and organizational security measures. As a result, there was a real risk of unauthorized access and disclosure of personal data for 188 individuals and 33 legal entities serviced by the accounting firm. This represents a “breach of confidentiality” within the meaning of Article 33 of the Regulation [26].

The main reason for the breach was the lack of adequate control over access to the schools’ information system. It is possible that the administration did not perform a comprehensive risk analysis before granting access to the external accounting firm. There might also be a lack of a clearly written information system security policy that includes mechanisms to limit access only to strictly necessary data. The accounting firm, for its part, is responsible for improper data storage, which led to the disclosure of personal information of clients and employees. This highlights the need for better control mechanisms in the processing of personal data by external organizations. The CPDP has imposed a monetary penalty on the accounting firm and a warning corrective measure on the private schools. This demonstrates a differentiation in responsibility between the two types of administrators, with the accounting firm being more severely sanctioned for the specific incident.

The analysis of the cases reviewed reveals several key issues in the field of personal data protection. The main problem is related to the lack of adequate mechanisms for control and protection of personal data. The publication of sensitive information (by the ISJC) and unsecured access (schools and accounting firm) reveal weaknesses in security management. A second issue is that personal data controllers have not conducted a detailed assessment of potential risks before taking certain actions, such as publishing declarations or providing access to external parties. In the case of the ISJC, the violation is due to the non-compliance with the data minimization principle, which led to unauthorized disclosure of information about judges, prosecutors, and their families. The hacker attack against the SAC and administrative courts shows that not only human errors but also external malicious actions can compromise information systems. This underscores the need for better incident response protocols.

While in the public sector (the ISJC, the SAC) there are weaknesses related to administrative pressure and insufficient control over published information, in the private sector (schools and accounting firm), the violations are mainly related to unsecured external access and poor practices in managing information infrastructure. In the cases of the ISJC and schools, the violation stems from management decisions, while the attack against the SAC

reveals technological vulnerabilities exploited by third parties.

Key takeaway: To enhance the effectiveness of personal data protection, several key measures need to be taken. Firstly, organizations should improve their technical security mechanisms by implementing automated systems for controlling published information and encrypting sensitive data. Additionally, regular audits and monitoring will help identify potential vulnerabilities and ensure timely response to incidents. Further, employee training in cybersecurity should be strengthened to minimize risks associated with human factors. This includes developing awareness programs about threats and implementing good practices for personal data protection. Finally, regulatory bodies should impose stricter penalties for systemic violations to ensure more effective compliance with legal requirements. Implementing these recommendations will contribute to significant improvements in risk management, both in the public and private sectors, and will minimize the likelihood of future incidents related to breaches of personal data protection.

c) Other Significant Data Breaches – Recommendations for Improvement

The identified gaps – including insufficient organizational preparedness, technical vulnerabilities, and lack of preventive measures – reveal the need for stricter regulatory intervention and investments in the security of information systems. It is particularly concerning that both human errors and malicious cyberattacks compromise sensitive information, underscoring the importance of a proactive approach to risk management. Effective implementation of technical measures, regular audits, and training to enhance cybersecurity are among the most necessary steps to minimize threats. Regulatory bodies also need to strengthen their sanctioning policy and apply proportional yet decisive measures against systemic violations. The introduction of stricter control mechanisms, as well as encouraging organizations to adhere to best practices, will be crucial for ensuring a high level of personal data protection in Bulgaria and within the context of European regulations.

Considering the analysis of all cases examined thus far, it becomes evident that there is a clear necessity to develop a unified model and a clearly defined algorithm for responding to personal data breaches, applicable to both the public and private sectors. This model should encompass minimum standards and action procedures, including technical and organizational measures, prevention methods, and effective incident response mechanisms. Creating and implementing such a unified approach should be a priority for future research and practical efforts in order to ensure a high level of personal data protection in compliance with European and national regulatory requirements.

CONCLUSIONS

In conclusion, it is evident that the organizations from the public and private sector in the Republic of Bulgaria have significant gaps in their internal processes related to handling data breaches. The analysed data breaches are a result of complex of factors such as insufficient technical and organisational measures implemented to ensure the security of the processed personal data, outdated technical equipment and information systems, lack of knowledge of the personnel how to react in such cases, missing internal procedures for reaction and data breach counteraction/consequence limitation, etc. It is evident that the organisations in Bulgaria need a working model defining clear algorithm how to react in case of data breaches and this will be subject to future work of the research team that co-authored the present analysis.

The analysis of the data breaches at Bulgarian Posts and the private bank underscores systemic weaknesses in both the public and private sectors when it comes to cybersecurity and data protection. One of the most pressing issues is the reliance on outdated IT infrastructure and the lack of proactive risk assessments, which make institutions vulnerable to cyberattacks. A key lesson from these cases is that organisations must prioritize continuous security evaluations and modernise their digital infrastructure to keep pace with evolving threats.

The above is also applicable to the case of the NRA data breach, with the additional reccomendations outlined in respect to the courts and the supervisory authority. Each data breach resulting from external actions must be carefully and thoroughly examined, including by technical experts, and any regulatory or judicial decisions on the appropriateness of technical and organisational mesures need to be specific, well-grounded and drafted after careful examination of all circumstances in order to comply with the views of the CJEU.

Furthermore, Bulgarian organizations must urgently adopt structured protocols for incident management and introduce mandatory cybersecurity training for their personnel. Regulatory oversight should be strengthened by ensuring regular compliance audits and imposing proportionate yet effective sanctions in case of systematic breaches. Addressing these areas proactively will significantly improve the resilience of both the public and private sectors against future cybersecurity incidents.

ACKNOWLEDGMENTS

The present paper was prepared as a result of the scientific research activities conducted within scientific project “Managing Personal Data Breach Response Processes in the Activities of Organisations in the Republic of Bulgaria” financed by the Bulgarian National Science Fund with the Ministry of Education“, “Competition for financing fundamental scientific research – 2024”, Contract No. КП-06-Н85/10 (BG-175467353-2024-11-0016-C01) dated 05.12.2024.

REFERENCES

[1] Official Journal of the European Union, L 119, pp. 1–88, May 4, 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj. [Accessed: Feb. 20, 2025].

[2] P. Voigt and A. von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International Publishing AG, 2017, p. 65.

[3] S. Room, "Security of Personal Data," in European Data Protection: Law and Practice, 3rd ed., E. Ustaran, Ed. Hyde Park Publishing Services: IAPP, 2023, p. 228.

[4] Commission for Personal Data Protection, Penal Order No 004/28.08.2019.

[5] Commission for Personal Data Protection, Decision No PPN-02-399/22.08.2019.

[6] Lex News, The court refused for the second time the agreement of the prosecution with Christian Boykov for "NRA Leaks", 01.11.2024 [Online]. Available: https://news.lex.bg. [Accessed: Feb. 20, 2025].

[7] Administrative Court Sofia City, Motion Order of 14.05.2021 rendered in Case 1037/2021, V Department.

[8] Commission for Personal Data Protection, Information Bulletin, vol. 5, no. 80, Sept. 2019. [Online]. Available: https://cpdp.bg/userfiles/file/Bulletin/KZLD_Bulletin_5_80_September_2019.pdf. [Accessed: Feb. 20, 2025].

[9] Sofia District Court, Decision of 26.10.2023, rendered in Case No 14811/2019.

[10] Administrative Court Sofia City, Decision No. 1247/26.02.2024, rendered in administrative case No. 12334/2023.

[11] Administrative Court Sofia City, Decision No. 565/02.02.2023, rendered in administrative case No. 10477/2019.

[12] Supreme Administrative Court, Decision No. 1398 of 07.02.2024 in administrative case No. 3781/2023, V Department.

[13] Supreme Administrative Court, Decision No. 9399 of 13.09.2021 in administrative case No. 11029/2020, II Department, Decision No. 9414 of 15.09.2021 in administrative case No. 9871/2020, III Department, Decision No. 9417 of 15.09.2021 in administrative case No. 11283/2020, III Department, Decision No. 9420 of 15.09.2021 in administrative case No. 10793/2020, III Department, Decision No. 9421 of 15.09.2021 in administrative case No. 8825/2020, III Department.

[14] Lex News, The court gave the go-ahead to a class action lawsuit against the NRA over the data leak, 27.11.2024 [Online]. Available: https://news.lex.bg. [Accessed: Feb. 20, 2025].

[15] Sofia District Court, Order No 348 of 10.01.2023, rendered in Case No 13344/2021, Appelate Court Sofia, Order No 549 of 28.02.2023, rendered in Case No 473/2023,

[16] Court of Justice of the European Union, Judgment of the Court (Third Chamber) of 14 December 2023 (request for a preliminary ruling from the Varhoven administrativen sad – Bulgaria) – VB v Natsionalna agentsia za prihodite, Case C-340/21, Natsionalna agentsia za prihodite.

[17] Commission for Personal Data Protection, Annual Report 2022. Sofia, Bulgaria: CPDP, 2022. [Online]. Available: https://cpdp.bg/wp-content/uploads/2023/11/Annual-report_2022_CPDP.pdf. [Accessed: Feb. 20, 2025].

[18] Administrative Court Sofia City, Court Decision No. 505/18.01.2024, rendered in administrative case No. 9929/2022.

[19] Commission for Personal Data Protection, Annual Report 2019. Sofia, Bulgaria: CPDP, 2019. [Online]. Available: https://cpdp.bg/userfiles/file/Annual%20Reports/Annual_Report_2019_CPDP.pdf. [Accessed: Feb. 20, 2025].

[20] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," *Cyber Security and Applications*, vol. 2, 100031, 2024. [Online]. Available: https://doi.org/10.1016/j.csa.2023.100031. [Accessed: Mar. 25, 2025].

[21] Administrative Court Sofia City, Court Decision No. 300/11.01.2024, rendered in administrative case No. 11485/2023.

[22] J. Martins, H. S. Mamede, and J. Correia, "Risk compliance and master data management in banking – A novel BCBS 239 compliance action-plan proposal," *Heliyon*, vol. 8, no. 7, e09627, 2022. [Online]. Available: https://doi.org/10.1016/j.heliyon.2022.e09627. [Accessed: Mar. 25, 2025].

[23] Lex News, A cyberattack has crashed the information system of all administrative courts, Jan. 27, 2025. [Online]. Available: https://news.lex.bg. [Accessed: Feb. 3, 2025].

[24] Lex News, A hacker group announced that it has the data leaked from the Supreme Administrative Court – publishing a portion as proof, Feb. 20, 2025. [Online]. Available: https://news.lex.bg. [Accessed: Feb. 22, 2025].

[25] Commission for Personal Data Protection, Annual Report 2019. Sofia, Bulgaria: CPDP, 2019. [Online]. Available: https://cpdp.bg/userfiles/file/Annual%20Reports/Annual_Report_2019_CPDP.pdf. [Accessed: Feb. 3, 2025].

[26] Commission for Personal Data Protection, Annual Report 2023. Sofia, Bulgaria: CPDP, 2023. [Online]. Available: https://cpdp.bg/wp-content/uploads/2024/03/Annual-report_2023_CPDP.pdf. [Accessed: Feb. 3, 2025].

Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 363-370

Implications of International Lawfare for the Global Security Architecture

Zhuliyan Zhelezov
Rakovski National Defence College
Sofia, Bulgaria
zhelezov@protonmail.com

***Abstrac*-The article analyses certain implications for global security architecture of using international law as an instrument of power by states in the digital age. The author's point of view is that in conditions of rising geopolitical competition, using international legal warfare to achieve strategic objectives increases the risks and threats for stability of international order. The scientific paper is divided into four sections. In the introduction, the main problem related to international lawfare is defined, including its significance for our international community. The first section defines a legal research methodology that is applied. The second conceptualizes international legal warfare. The third examines different cases of lawfare that have negative implications for global security architecture. The fourth deals with emerging and disruptive technologies that define geopolitical competition and how they relate to lawfare. In the conclusion, an assessment is provided regarding developments of international law, including its normative role for the global security architecture. The paper makes few recommendations for preservation of current international order, which is being challenged by the growing number of legal warfare practices between various geopolitical actors.**

Keywords- Arms Control, Emerging and Disruptive Technologies, Global Security Architecture, Lawfare

I.INTRODUCTION

In conditions of resource depletion and changing international order, the strategic competition between states is increasing [1]. New powerful actors emerge in the Global South, which challenge the geopolitical status quo. They demand a greater share in the global governance, as well as a stronger role in the global financial system. Meanwhile, the emerging and disruptive technologies (EDT) are changing the nature of state confrontation, including the means and methods of warfare. International actors are using old and new instruments of national power to achieve strategic advantage [2] over their opponents. International law is instrumentalized and misused in order to consolidate or undermine established relations of power [3].

However, using the international legal system as an instrument of power or as a catalyst to achieve national strategic objectives, undermines the main role and purpose of international law, which is to regulate the relations between states. Since international law is becoming ineffective in resolving interstate issues, countries are increasingly referring to hard power-based mechanisms for resolving their disputes. The implications of this negative trend are an increased militarization of international relations and emergence of new risks and threats to the global security architecture. The most relevant case in point of legal warfare (lawfare) is the intentional dismantlement of several arms control treaties during the last decade by states in order to gain strategic advantage over their competitors. In a digital era of EDT, removing the mutually agreed upon restraints on specific weapons or the infringement of legal norms, related to global security, is even more dangerous than the times of the Cold War, and might cause serious military consequences for the international order and the humankind.

II.MATERIALS AND METHODS

The study applies a legal research methodology, including doctrinal research and legal scholarship. Doctrinal research as a legal method is employed to systematize, interpret, and clarify the law pertaining to several cases of international lawfare by analysing authoritative texts. Primary legal sources include the UN Charter, the UN Convention on the Law of the Sea (UNCLOS), the Outer Space Treaty (OST), the Comprehensive Nuclear-Test-Ban Treaty (CTBT), the Measures for the Further Reduction and Limitation of Strategic Offensive Arms (New START), and the Intermediate-Range Nuclear Forces (INF) Treaty, as well as case law of the International Court of Justice (ICJ). Secondary legal sources include the Journal of Strategic Studies, the Journal of National Security Law and Policy, the Journal on Baltic Security, the Journal on the Use of Force and International Law, as well as publications from authoritative think tanks such as the RAND Corporation, the Center for Strategic and International Studies, the

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8463
© 2025 The Author(s). Published by RTU PRESS.
This is an open-access article under the Creative Commons Attribution 4.0 International License.

Stockholm International Peace Research Institute (SIPRI), the Institut français des relations internationals, etc.

The study applies empirical legal scholarship in which qualitative methods from international relations are combined and employed, including content analysis, case selection, and process tracing in order to assess the implications of lawfare for international security system in the 21st century. Empirical arguments are provided in order to highlight the normative points made in the article.

III. RESULTS AND DISCUSSION

A. Defining International Lawfare

International law is the product of aspiration of international community to establish world order, wherein each country is able to realize peacefully its national interests and its full potential, as well as to interact in a constructive manner with other states [4]. In other words, the regulative role of international law is based on the perception and consensus of all states that certain rules and principles must be observed, since the whole global community benefits from this.

In light of the foregoing, international law is a symbol of hope and desire of humankind for peace. Whatever its shortcomings, it exists as a promise to establish justice and as a motivating factor for the realization of political transformation [5] on a global scale. Further, international law provides weaker states with an opportunity to file claims before courts against stronger countries, as well as to compete with them in the legal domain on equal basis. In this regard, it is a standard for criticism against power politics and a means of protecting infringed interests. However, international law is also used as an instrument of power, supporting the realization of national interests and geopolitical ambitions of particular state leaders.

International lawfare corresponds with the last purpose mentioned hereinabove. It is defined as the use of an international legal system to establish, perpetuate, or amend power relations in order to counter an adversary [6] and disrupt its actions. This is achieved by overcoming legal constraints through reinterpreting existing rules of law. Another way is by virtue of creating new norms or by means of using international litigation to achieve a strategic effect. Finally, international law can be utilized to inflict reputational damages to the opponent [6, pp. 10-15]. An important feature of lawfare is that the use or misuse of the international legal system should be a substitute for traditional military means [7] or to complement them. Therefore, in order to define a legal act as lawfare, it is mandatory to be in relation to ongoing military activity. It can be applied on the tactical, operational, and strategic level [8].

Nonetheless, some authors claim that lawfare might have a positive connotation. For instance, using lawfare instead of military means can reduce the destructiveness of war [7] or at least its intensity. Furthermore, lawfare can serve weaker states as a tool for overcoming material and power inequality against their stronger foes. This is achieved through strategic litigations, since the parties to a lawsuit are equal before the law and before the court.

International law has evolved throughout the time – from practices based on the code of chivalry to becoming a crucial element in defining strategic competition and modern warfare [9] in the 21st century. In the past, it was narrowly used to assess what is permitted and what is forbidden during a conflict. Nowadays, it is often applied by states as a mode of warfare to legitimize or challenge certain activities in condition of strategic competition in order to achieve advantage against their opponents, as well as to justify the use of force (jus ad bellum) or the conduct of hostilities (jus in bello) in armed conflicts.

Lawfare is often included in information and psychological operations in order to strengthen certain claims and narratives. In other words, nowadays, the legal preparation of the battlefield, as well as using legal systems during the conflict, are of crucial importance for the success of the political and/or military strategy in terms of the ability of the state leadership to legitimize a military operation or a geopolitical project in order to gain societal support. Lawfare leverages activities within the legal "grey zone", wherein it is extremely difficult to apply basic norms and principles related to strategic deterrence, harnessing cutting-edge technologies or the use of force [10].

Further, EDT has accelerated states' capabilities to use the legal "grey zone" in order to achieve their national objectives, thus making these legal challenges the norm, rather than the exception [10]. For instance, malicious activities of states in cyber space are highly difficult to attribute to. Moreover, lawfare is employed by states even out of the legal "grey zone", where international norms and principles are being violated for the sake of strengthening strategic deterrence or improving communication capabilities. However, such cases of international lawfare in conditions of global militarization [11] and EDT generate new risks for the global security architecture.

B. Cases of International Lawfare with Negative Implications for the Global Security Architecture

China has developed the most sophisticated lawfare strategy in the world within the framework of its "Three Warfares" concept. The Chinese leadership perceives legal warfare as an instrument of power that is capable of strengthening the geopolitical initiatives or supporting potential war efforts [12] of the country. For instance, Beijing's expansionist strategy in South China Sea is based on combination of lawfare tactics and nationalist misinterpretation of history. The Chinese leadership has made several legal claims regarding sovereignty and territorial rights over disputed islands and archipelagos in South China Sea such as the Paracel and Spratly Islands. Meanwhile, Beijing has ignored the South China Sea Arbitration award [13], which concluded that China's claims have no sufficient legal grounds under the UNCLOS. Further, Beijing is expanding its Exclusive Economic Zone (EEZ) through the creation of artificial islands on top of coral reefs, which subsequently militarizes, thus violating the EEZ of other countries in the region and undermining the limitations stipulated in

UNCLOS. Meanwhile, China claims that according to international law, foreign military activities in its EEZ, such as reconnaissance flights, are forbidden.

The purpose of China's lawfare strategy regarding UNCLOS is to consolidate Beijing's control over South China Sea [14] and its abundant resources. However, this approach in a region of geostrategic importance such as South China Sea, might have enormous negative military consequences, since Chinese lawfare is directed towards challenging the USA military presence in the area, thus increasing the risk of serious incidents between two nuclear powers [3, p. 13-17].

Another case of lawfare is China's active engagement in establishing the legal framework that will govern outer space activities in the next decades. Beijing perceives it as a strategic domain for future competition with other states such as Russia and the USA, where harnessing advanced space technologies will lead to advantages [15]. Space activities are governed by the OST, which only stipulates the main principles and basic rules of law. It defines the exploration and utilization of outer space to be for the benefit and in the interests of the humankind. As per the OST, outer space shall be free for exploration and use by all countries and shall not be a subject to national appropriation by claims of sovereignty. Furthermore, OST prohibits the placement of nuclear weapons or other weapons of mass destruction in orbit or on celestial bodies. Therefore, the limited body of international law in this field provides China with opportunities to engage and shape the normative dialogue regarding future space regulations in its own interest.

By virtue of lawfare, China's assertion of sovereignty over outer space above its national territory aims at countering or controlling the satellites overflown over the state [16]. However, claims of "vertical sovereignty" is in contradiction to OST [17, p. 168], since it restricts the freedom of action of other states in outer space. Furthermore, on false legal grounds of self-defence (art. 51 of the UN Charter), Beijing is actively improving its counterspace weapons capabilities and has implemented reforms to integrate more effectively cyberspace, space and electronic warfare into joint military operations [16, p. 464].

The Chinese perception of sovereignty also extends to cyber security, thereby including the protection of both the technology and the actual data transmitted and stored across the Internet. The government has imposed strict regulations in order to control and monitor the internet resources and data traffic. However, this approach goes in contradiction to China's practice of harvesting data from other states, conducting cyber operations, thereby establishing a double-standard that makes it difficult to predict if Beijing is going to comply or not with international law [18]. Moreover, the Chinese leadership has refused on many occasions to recognize that international law, including jus ad bellum and jus in bello, applies to cyberspace [17, p. 169].

The gravest challenge for the international order in the 21st century stems from Russia's pursuit of great power status through force and use of legal warfare. In order to achieve its geopolitical objectives, the Kremlin is undermining basic legal principles such as the obligation to comply with international treaties and the inviolability of national borders in Europe [19]. Moscow is also eroding nuclear norms and institutions [20].

Russia has used on several occasions lawfare to make territorial, political, and economic claims against its neighbouring countries (Moldova, Georgia, Ukraine). The Russian leadership has tried to advance a legal justification for its use of force against Ukraine in order to receive support from the international community and its own population. However, the Russian legal claims (self-defence, humanitarian intervention, etc.) failed on multiple grounds. The Russian "special military operation" in Ukraine constitutes an unlawful use of force [21], which can be defined as an act of aggression and a grave breach of article 2 (4) of the UN Charter which is a jus cogens norm with erga omnes effects. In terms of jus in bello, during the armed conflict, Russia has perpetrated a wide range of war crimes, including the intentional targeting of civilians and critical infrastructure [22].

Furthermore, Moscow has ignored the ICJ provisional measures order to immediately suspend its military operations in the territory of Ukraine [23], as well as ICJ's judgement, confirming Russia's international law breaches, including the failure to investigate terrorism financing and the suppression of Ukrainian language and culture in Crimea [24]. Moscow has also ignored the International Criminal Court's (ICC) arrest warrants against representatives of the Russian military and political leadership on the grounds that the Kremlin does not recognize the ICC's jurisdiction. In accordance with the responsibility of states for internationally wrongful acts, the West has taken collective countermeasures against Russia, including but not limited to the blocking of around $300 billion of sovereign Russian assets [25]. Moscow has tried to unblock a significant part of them by virtue of lawfare, including through strategic litigation, but to this day its attempts are unsuccessful [26].

Russia employs lawfare as part of its strategic deterrence policy against the West. For instance, on 19 November 2024, the Kremlin approved new nuclear doctrine, lowering the nuclear threshold as a signal to the West [27]. Further, the Kremlin withdrew its ratification of the CTBT, which prohibits all nuclear explosions, whether for military or for peaceful purposes. It suspended the New START treaty last year, which reduces nuclear arms between the US and Russia, and establishes a limit on deployed strategic warheads. Before that Moscow breached the INF Treaty, which had stipulated the prohibition of all US and Soviet missiles with ranges between 500 and 5,500 kilometres.

In light of the foregoing, Russia's lawfare in arms control undermines nuclear institutions and norms, including nonproliferation, nonuse, and nontesting [20, p.

4], thus increasing the risks for the global security architecture. On the other hand, Russia continues to pretend that it is adhering to arms control treaties, while modernizing its nuclear capabilities and escalating nuclear threats in order to advance its objectives in the war in Ukraine [28].

Through lawfare Russia exploits successfully UNCLOS norms in order to increase its influence and sovereignty rights in the Arctic area. Moscow perceives the region as being of strategic importance for its defence planning and economic development, thus rebuilding its military capabilities and modernizing its regional military infrastructure [29]. Meanwhile, the Kremlin had made a claim to the Commission on the Limits of the Continental Shelf (CLCS) regarding North Pole territory. These claims have significantly increased its limits of the continental shelf beyond 200 M from the baselines in respect of the Arctic Ocean. While the CLCS did not approve the entirety of the approximate 2 million square kilometres claimed by the Russian Federation, the submission to a great extent was approved in February 2023, rejecting only approximately 300 000 square km of claimed entitlement [30]. The Russian claim collides with sovereignty demands of Greenland/Denmark and Canada, especially regarding the Lomonosov Ridge area. Even though the dispute is not resolved, and the recommendations of CLCS are not legally binding, they have normative value, since the Kremlin's claim is recognized by the highest international authority in the field.

Russia's lawfare strategy is aimed at influencing the polar governance in its favour in the long-term, including the ability to exercise control, claim sovereignty rights over the Northern Sea Route, and generate denial capabilities [29]. However, this highly securitized and militarized approach to the Arctic area has direct negative consequences for other polar nations such as Canada, Denmark, Finland, Norway, Sweden, and US, which have experienced infringement of their maritime rights by Russia and are being engaged in another area of competition.

Furthermore, the Kremlin applies lawfare in the UN Security Council (UNSC) to advance its own interests. For instance, Moscow's decision to exercise a veto in March 2024 against the United Nations' renewal of the panel of UN experts blocks the ability of the international community to monitor North Korea's compliance with international sanctions. Deepening Russia-North Korea relations, including via a new revised security alliance [31], would encourage Pyongyang to continue endangering the global security architecture by virtue of nuclear threats and the development of long-range ballistic missiles.

While the US does not have a clear lawfare strategy like China or Russia, it has resorted to legal techniques in order to deal with foreign policy challenges in the past. In fact, there are several attempts to conceptualize, operationalize and legitimize lawfare in the US in order to create legal combat capabilities [32]. The decision of Washington to withdraw from the Treaty on Open Skies in 2020 and from the INF treaty in 2019 is an example of lawfare which aimed at addressing non-compliance issues with Russia. The Treaty on Open Skies allowed the parties, including the US and Russia, to operate unarmed observation flights over one another's territory. Even though Washington's actions had been provoked by Russia's intentional and systematic violations of these treaties, they had a huge negative impact on the arms control efforts of the international community.

The US employs lawfare by targeting geopolitical competitors with financial and economic sanctions [3], including China, Iran, Cuba, Venezuela, Russia, etc. These coercive measures have a significant negative effect on GDP growth and consumption in the targeted countries, as well as on their trade and foreign direct investments [33]. However, sanctions on such a scale as observed nowadays, might cause negative shocks within the world economy, capable of disrupting global supply chains and increasing costs for consumers and businesses the world over.

Lawfare has also been used by weaker states against their stronger competitors. For instance, during the war, Ukraine has employed strategic litigation against Russia as a lawfare tactic. It has filed two cases at the ICJ and two arbitrations before the International Tribunal for the Law of the Sea. ICC investigations are also underway, as well as efforts to isolate Moscow from international institutions. Ukraine is also using domestic courts to prosecute Russian war criminals and to provide the international community with information regarding Russia's violations of jus in bello. Furthermore, certain steps are being taken towards creating a Special Tribunal for the Crime of Aggression against Ukraine, within the framework of the Council of Europe.

Another example of lawfare is Palestine's inter-State communication against Israel before the Committee on the Elimination of Racial Discrimination with regard to Israel's conduct in the Occupied Palestinian Territory (OPT). Moreover, in a nonbinding advisory opinion, in July 2024, ICJ ruled out in favour of Palestine that Israel's continued presence in the OPT is unlawful [34] and must be ceased.

The abovementioned cases of lawfare do not occur in a vacuum. They are interrelated and emerge in a digital era of fast-paced technological development, wherein states compete and cooperate with each other in order to secure resources and new technologies, including in the military domain.

C. Lawfare in Conditions of Emerging and Disruptive Technologies

Technological progress has defined every aspect of our lives. In the digital age, EDT such as big data, artificial intelligence (AI), blockchain, cloud-based solutions, and automation, have a profound effect on the business, economy, interstate relations, and on human interactions all over the world. On the one hand, these technologies can contribute for the realization of global sustainable development goals. In reference to security and defense, EDT are perceived as crucial components of national, institutional and economic growth, contributing to the

realization of strategic autonomy, technological and digital sovereignty, necessary for survival of the state [35].

On the other hand, EDT are capable of eroding global security architecture if applied for malicious purposes. States are engaged in a competition in the field of innovation and breakthrough capabilities [36]. As a result, certain risks from the application of EDT have emerged for the global security architecture, as well as new dilemmas regarding strategic deterrence [37, p. 5]. EDT are defined as cutting-edge technological innovations capable of resolving sophisticated security and defence matters and providing strategic, operational or tactical advantage against the competitor [38], thus revolutionizing military affairs.

Lawfare and EDT are intertwined. States wage lawfare to create and/or influence governing mechanisms that are meant to deal with EDT in the future. The main objectives might include securing better positions in terms of creating new and interpreting existing rules of law, which govern contested domains such as cyber or outer space; protecting own high-tech companies; ensuring better access to global supply chains, thus ensuring the flow of critical materials and resources necessary for technological development [39], [40].

Meanwhile, the application of EDT by states in most of the cases is situated within the "grey zone" of international law, since rules of engagement are weak or do not exist. In other words, while there is no international legal framework that govern disruptive technologies [41], different geopolitical actors are exploiting this opportunity. For instance, cyber-attacks, initiated by Russia and China, against digitalized critical infrastructure, are difficult to attribute. And if successfully attributed, there is no law-enforcement mechanism to be applied against them. Further, there is no comprehensive legal framework, regulating "dual activities" in outer space, examples of which are Beijing's pursuit of space and counterspace capabilities [42] and its exploitation of maritime "grey" zone situations in South China Sea [43]. There is no universal consensus on a legal regime governing the use of generative AI, which can be exploited for spreading disinformation and propaganda by states such as China [44] and Russia.

As part of EDT, the development of quantum computing capabilities can also be subsumed under the "grey zone" of international law. Harnessing the potential of quantum technologies can provide a state with the ability to read encrypted information transferred over the internet, thus obtaining access to critically sensitive information and securing strategic advantage over its opponents [45].

IV. Conclusions

International law has structural problems that should be addressed in an urgent manner. At the moment, the UN system is not capable of managing global security matters. Key UN institutions such as the ICJ and the UNSC are unreformed since 1945, as well as the UN Charter provisions on the peaceful settlement of disputes [46]. As a result, the propensity of states to refer to hard power-based methods and violence instead of international law to solve their contested matters is increasing. Revisionist powers such as Russia, China, and North Korea demonstrate willingness and resoluteness to undermine international law or misuse it for their own benefit. Meanwhile, the US is ready to wage lawfare in order to deter them.

Although there is a notion that lawfare can operate as a positive "good" [7], the author's point of view is that the more often states refer to legal warfare to achieve their strategic objectives, the greater the risks and threats become for the stability of international order. This applies especially in times of increasing geopolitical competition between leading powers, as we are witnessing today. This hypothesis has been tested and proven by the factual impact on the global security architecture of the aforementioned cases of Russian, Chinese, and American lawfare, as well as by the numbers from SIPRI's Military Expenditure Database.

First, Russia's legal warfare is likely to have the strongest negative impact on nuclear norms and institutions, as well as on the prohibition of the use of force in international relations. The Chinese lawfare gravely affects the maritime order that preserves the freedom of the seas, while the American legal warfare disrupts supply chains and create trade barriers on a global scale.

Second, the increasing number of legal warfare cases during the last decade indicates that more states perceive international law as an instrument of power, which is not effective enough or capable of resolving interstate disputes in security, economy, maritime matters, etc. As a result, geopolitical actors more often refer to hard power-based methods to deal with their enemies and competitors. This negative trend has been statistically proven by the fact that the world military expenditure increased for the ninth consecutive year in 2023, reaching a total of 2 443 billion USD [11].

Overall, the potential for a global catastrophic risk has been increasing in recent years and appears likely to increase in the coming decade [47]. International law should be reinvented and legal culture has to be improved in order to meet these challenges and to manage the tectonic geopolitical shifts in the balance of power, including the strategic competition between the leading states of the day. Critical institutions of the UN system must be reformed in order to receive more legitimacy. At the moment, a lot of states are no longer believing in the absolute benefits of global cooperation, but are increasingly concerned that they are gaining less from the international order than others [48].

A good starting point for reforms should be to transfer more powers related to security matters from the UNSC to the UN General Assembly in order to overcome the current deadlock [48]. Furthermore, an entirely new structure within the UN system, dealing with risk escalation management, based on global consensus, should be established and enabled as soon as possible. Last but not least, the international community has to create a legal

framework for the initiation of a dialogue on strategic stability between all nuclear powers.

In an era of fast-paced technological developments and geopolitical competition, international law should be a driving force in defining a legal and ethical framework to minimize the negative effect of EDT on the global security architecture. International legal regimes and standardization are necessary in the fields of big data, quantum technologies, generative AI, bio-, nano-, geospatial technology, blockchain, cloud-computing, FinTech, etc. The "Soft Law" instruments should play an important role in this process, since they are more flexible than "hard law" in achieving consensus on such contested matters.

Further, states must strengthen the concept of compliance (rule of observance) in international law. They should make extra efforts to uphold and reinforce nuclear norms in order to address the risk of weakening arms control in the context of EDT [20]. Moreover, new rules and principles of law protecting the development of technical standards in EDT, from malicious influence should be created and respected.

The international community should achieve consensus on the existence and validity of jus cogens norms with universal legal force and legally binding effect. Well-timed and resolute collective countermeasures must be adopted all the time, when states decide to wage lawfare and perpetrate grave breaches of these norms. This would have a legitimizing and strengthening effect on international law. However, ignoring one's systemic violations of imperative international rules and principles might motivate others to follow suit, which has the potential to bring the humankind back to the Hobbesian state of nature.

REFERENCES

[1] M. J. Mazarr, "Understanding competition. Great Power Rivalry in a Changing International Order - Concepts and Theories," *RAND Corporation*, March 2022. [Online]. Available: https://www.rand.org/pubs/perspectives/PEA1404-1.html [Accessed November 03, 2024].

[2] G. Elefteriu, W. Freer, and J. Rogers, "What is Strategic Advantage?," *Council of Geostrategy*, November 2023. [Online]. Available: https://www.geostrategy.org.uk/research/what-is-strategic-advantage/?cmplz-force-reload=1730636254400 [Accessed November 03, 2024].

[3] J. C. Pinos and M. F. Hau, *Lawfare. New Trajectories in Law*. London: Routledge, 2023.

[4] M. E. O'Connell, *The Power & Purpose of International Law: Insights from the Theory & Practice of Enforcement*. New York: Oxford University Press, 2008.

[5] M. Koskenniemi, "What Is International Law For?" in *International Law*, M. Evans, Ed. New York: Oxford University Press, 2018, pp. 28-50.

[6] A. Ferey, "Towards a War of Norms? From Lawfare to Legal Operations," *Institut français des relations internationales*, April 2022.

[7] C. J. Dunlap, Jr., "Lawfare Today: A Perspective," *Yale Journal of International Affairs*, Winter 2008, pp. 146-154.

[8] L. Sanders, "Lawfare in the 21st century," in *Routledge Handbook of the Future of Warfare*, A. Gruszczak and S. Kaempf, Eds. New York: Routledge, 2024, 109-119.

[9] D. Kuwali, "Local Conflict, Global Impact: Lawfare in Warfare," *Raoul Wallenberg Institute*, September 2024. [Online]. Available: https://rwi.lu.se/blog/local-conflict-global-impact-lawfare-in-warfare/ [Accessed November 14, 2024].

[10] R. Brooks, "Rule of Law in the Gray Zone," *Modern War Institute at West Point*, February 2018. [Online]. Available: https://mwi.westpoint.edu/rule-law-gray-zone/ [Accessed November 14, 2024].

[11] N. Tian, D. L. Da Silva, X. Liang, and L. Scarazzato, "Trends in World Military Expenditure, 2023," *Stockholm International Peace Research Institute*, April 2024. [Online]. Available: https://www.sipri.org/sites/default/files/2024-04/2404_fs_milex_2023.pdf [Accessed November 14, 2024].

[12] S. Lee, "China's 'Three Warfares': Origins, Applications, and Organizations," *Journal of Strategic Studies*, vol. 37, no. 2, pp. 198-221, April 2014. [Online]. Available: https://doi.org/10.1080/01402390.2013.870071 [Accessed November 14, 2024].

[13] The Republic of Philippines v. The People's Republic of China, *Permanent Court of Arbitration*, Case number 2013–19, pp. 471-477, July 2016. [Online]. Available: https://pcacases.com/web/sendAttach/2086 [Accessed November 16, 2024].

[14] D. Guilfoyle, "The rule of law and maritime security: Understanding lawfare in the South China Sea," *International Affairs*, vol. 95, no. 5, pp. 999-1017, May 2019. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3378904 [Accessed November 16, 2024].

[15] D. Cheng, "China and Space: The Next Frontier of Lawfare," *United States Institute of Peace*, August 2023 [Online]. Available: https://www.usip.org/publications/2023/08/china-and-space-next-frontier-lawfare [Accessed November 16, 2024].

[16] B. A. White, "Reordering the Law for a China World Order: China's Legal Warfare Strategy in Outer Space and Cyberspace," *Journal of National Security Law & Policy*, vol. 11, no. 435, pp. 435-488, June 2021. [Online]. Available: https://jnslp.com/wp-content/uploads/2021/06/Reordering-the-Law-for-a-China-World-Order_2.pdf [Accessed November 16, 2024].

[17] O. F. Kittrie, *Lawfare. Law as Weapon of War*. Oxford: Oxford University Press, 2016.

[18] J. Foley, "Multi-Domain Legal Warfare: China's Coordinated Attack on International Rule of Law," *Lieber Institue at West Point*, May 2024. [Online]. Available: https://lieber.westpoint.edu/multi-domain-legal-warfare-chinas-coordinated-attack-international-rule-law/ [Accessed November 16, 2024].

[19] M. Voyger, "Russian Lawfare – Russia's Weaponisation Of International And Domestic Law: Implications For The Region And Policy Recommendations," *Journal on Baltic Security*, vol. 4, no. 2, pp. 35-42, December 2018. [Online]. Available: https://journalonbalticsecurity.com/journal/JOBS/article/54/info [Accessed November 16, 2024].

[20] H. Williams and D. Horschig, "House of Cards? Nuclear Norms in an Era of Strategic Competition," *Center for Strategic and International Studies*, July 2018. [Online]. Available: https://www.csis.org/analysis/house-cards [Accessed November 16, 2024].

[21] J. A. Green, C. Henderson, and T. Ruys, "Russia's attack on Ukraine and the jus ad bellum," *Journal on the Use of Force and International Law*, vol. 9, no. 1, pp. 4-30, March 2022. [Online]. Available: https://doi.org/10.1080/20531702.2022.2056803 [Accessed November 16, 2024].

[22] A. S. Bowen and M. C. Weed, "War Crimes in Ukraine," Congressional Research Service, Report № R47762, Washington, October 2023. [Online]. Available:

https://crsreports.congress.gov/product/pdf/R/R47762 [Accessed November 16, 2024].

[23] Allegations of Genocide under the Convention on the Prevention and Punishment of the Crime of Genocide (Ukraine v. Russian Federation), *International Court of Justice*, Request for the Indication of Provisional Measures, Order of 16 March 2022. [Online]. Available: https://www.icj-cij.org/node/106135 [Accessed November 16, 2024].

[24] Application of the International Convention for the Suppression of the Financing of Terrorism and of the International Convention on the Elimination of All Forms of Racial Discrimination (Ukraine v. Russian Federation), *International Court of Justice*, Judgement of 31 January 2024. [Online]. Available: https://www.icj-cij.org/node/203473 [Accessed November 16, 2024].

[25] E. Fabrichnaya and G. Faulconbridge, "What and where are Russia's $300 billion in reserves frozen in the West?" *Reuters*, December 2023. [Online]. Available: https://www.reuters.com/world/europe/what-where-are-russias-300-billion-reserves-frozen-west-2023-12-28/ [Accessed November 18, 2024].

[26] NKO AO National Settlement Depository v Council of the European Union, *General Court of the European Union*, Judgment in Case T-494/22, September 2024. [Online]. Available: https://curia.europa.eu/juris/documents.jsf?num=T-494/22 [Accessed November 18, 2024].

[27] G. Faulconbridge and A. Kolodyazhnyy, "Putin issues warning to United States with new nuclear doctrine," *Reuters*, November 2024. [Online]. Available: https://www.reuters.com/world/europe/putin-issues-warning-us-with-new-nuclear-doctrine-2024-11-19/ [Accessed November 19, 2024].

[28] H. Williams, K. Hartigan, L. MacKenzie, and R. Younis, "Russian Nuclear Calibration in the War in Ukraine," *Center for Strategic and International Studies*, February 2024. [Online]. Available: https://www.csis.org/analysis/russian-nuclear-calibration-war-ukraine [Accessed November 16, 2024].

[29] M. Boulègue, "The militarization of Russian polar politics," *The Royal Institute of International Affairs*, October 2023. [Online]. Available: https://www.chathamhouse.org/2022/06/militarization-russian-polar-politics/summary [Accessed November 18, 2024].

[30] B. Kunoy, "Recommendations on the Russian Federation's Proposed Outer Continental Shelf in the Arctic Area," *Blog of the European Journal of International Law*, March 2023. [Online]. Available: https://www.ejiltalk.org/recommendations-on-the-russian-federations-proposed-outer-continental-shelf-in-the-arctic-area/ [Accessed November 18, 2024].

[31] V. Cha and E. Kim, "The New Russia-North Korea Security Alliance," *Center for Strategic & International Studies*, June 2024. [Online]. Available: https://www.csis.org/analysis/new-russia-north-korea-security-alliance [Accessed November 19, 2024].

[32] J. Williams, "Legitimizing and Operationalizing US Lawfare: The Successful Pursuit of Decisive Legal Combat in the South China Sea," *Journal of Indo-Pacific Affairs*, December 2020. [Online]. Available: https://www.airuniversity.af.edu/JIPA/Display/Article/2452650/legitimizing-and-operationalizing-us-lawfare-the-successful-pursuit-of-decisive/ [Accessed February 01, 2025].

[33] J. Gutmann, M. Neuenkirch, and F. Neumeier, "The economic effects of international sanctions: An event study," *Journal of Comparative Economics*, vol. 51, no. 4, pp. 1214-1231, December 2023. [Online]. Available: https://doi.org/10.1016/j.jce.2023.05.005 [Accessed February 01, 2025].

[34] Legal Consequences arising from the Policies and Practices of Israel in the Occupied Palestinian Territory, including East Jerusalem - The Court gives its Advisory Opinion and responds to the questions posed by the General Assembly, International Court of Justice, 19 July 2024. [Online]. Available: https://www.icj-cij.org/sites/default/files/case-related/186/186-20240719-pre-01-00-en.pdf [Accessed February 01, 2025].

[35] R. Csernatoni, "The EU's hegemonic imaginaries: from European strategic autonomy in defence to technological sovereignty," *European Security*, vol 31, no. 3, pp. 395-414, September 2022. [Online]. Available: https://doi.org/10.1080/09662839.2022.2103370 [Accessed November 19, 2024].

[36] S. Adorf, A. Knack, B. Ohara, and M. Shizu, "Exiting Normal: Emerging Disruptive Technologies and their Impact on Military Operations and Equipment," *GLOBSEC Policy Institute & Sasakawa Peace Foundation*, September 2021. [Online]. Available: https://www.globsec.org/what-we-do/publications/exiting-normal-emerging-disruptive-technologies-and-their-impact-military [Accessed November 18, 2024].

[37] J. Bergeron, "Emerging disruptive technologies: Dilemmas of deterrence," *Council on Geostrategy*, May 2024. [Online]. Available: https://www.geostrategy.org.uk/research/emerging-disruptive-technologies-dilemmas-of-deterrence/ [Accessed November 18, 2024].

[38] R. Csernatoni and B. O. Martins, "Disruptive Technologies for Security and Defence: Temporality, Performativity and Imagination," *Geopolitics,* vol. 29, no. 3, pp. 849-872, June 2023. [Online]. Available: https://doi.org/10.1080/14650045.2023.2224235 [Accessed November 19, 2024].

[39] D. Criekemans, "Geotechnical Ensembles: How New Technologies Change Geopolitical Factors and Contexts in Economy, Energy, and Security," in *Geopolitics and International Relations. Grounding World Politics Anew*, D. Criekemans, Ed. Leiden: Brill, 2023, pp. 61-96.

[40] G. Csurgai, "The Increasing Importance of Geoeconomics in Power Rivalries: From the Past to the Present," in *Geopolitics and International Relations. Grounding World Politics Anew*, D. Criekemans, Ed. Leiden: Brill, 2023, pp. 244-257.

[41] T. Christou and I. Walden, "Legal and Regulatory Implications of Disruptive Technologies in Emerging Market Economies," *Centre for Commercial Law Studies*, August 2018. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3230674 [Accessed November 19, 2024].

[42] A. Schaffer and K. Bingen, "Engaging China on Space with Eyes Wide Open," *Center for Strategic & International Studies,* October 2024. [Online]. Available: https://www.csis.org/analysis/engaging-china-space-eyes-wide-open [Accessed November 18, 2024].

[43] Y. Shinji, Y. Masaaki, and M. Rira, "China's Quest for Control of the Cognitive Domain and Gray Zone Situations," *National Institute for Defense Studies, Japan*, 2023. [Online]. Available: https://www.nids.mod.go.jp/publication/chinareport/pdf/china_report_EN_web_2023_A01.pdf [Accessed November 21, 2024].

[44] N. Beauchamp-Mustafaga, K. Green, W. Marcellino, S. Lilly, and J. Smith, "Dr. Li Bicheng, or How China Learned to Stop Worrying and Love Social Media Manipulation. Insights Into Chinese Use of Generative AI and Social Bots from the Career of a PLA Researcher," *RAND Corporation*, October 2024. [Online]. Available: https://www.rand.org/pubs/research_reports/RRA2679-1.html [Accessed November 20, 2024].

[45] E. Parker, "When a Quantum Computer Is Able to Break Our Encryption, It Won't Be a Secret," *RAND Corporation*, September 2023. [Online]. Available: https://www.rand.org/pubs/commentary/2023/09/when-a-quantum-computer-is-able-to-break-our-encryption.html [Accessed November 18, 2024].

[46] A. Lopez-Claros, A. L. Dahl, and M. Groff, *Global Governance and the Emergence of Global Institutions for the 21st Century*. Cambridge: Cambridge University Press, 2020, pp. 208-235.

[47] H. H. Willis *et al*., "Global Catastrophic Risk Assessment," *RAND Corporation*, October 2024. [Online]. Available: https://www.rand.org/pubs/research_reports/RRA2981-1.html [Accessed November 20, 2024].

[48] T. Bunde, S. Eisentraut, and L. Schütte, "Munich Security Report, 2024: Lose-Lose?" Presented at the Munich Security Conference 2024, Munich, Germany, February 2024. [Online]. Available: https://securityconference.org/en/publications/munich-security-report-2024/ [Accessed November 18, 2024].

[49] R. Gowan, "The UN Security Council between Rifts and Reform," *International Crisis Group*, July 2023. [Online]. Available: https://www.crisisgroup.org/global/un-security-council-between-rifts-and-reform [Accessed November 19, 2024].