

RĒZEKNES TEHNOLOĢIJU AKADĒMIJA  
Inženieru fakultāte

REZEKNE ACADEMY OF TECHNOLOGIES  
Faculty of Engineering

# **VIDE. TEHNOLOĢIJA. RESURSI**

XV starptautiskās zinātniski praktiskās konferences rakstu krājums  
2024.gada 27.-28.jūnijs

**4.SĒJUMS**

# **ENVIRONMENT. TECHNOLOGY. RESOURCES**

Proceedings of the 15<sup>th</sup> International Scientific and Practical Conference  
June 27<sup>th</sup> – 28<sup>th</sup>, 2024

**Volume IV**

Rēzekne  
2024

**VIDE. TEHNOLOĢIJA. RESURSI.** 15.starptautiskās zinātniski praktiskās konferences materiāli. 2024.gada 27.-28. jūnijs. 4.sējums: Rēzeknes Tehnoloģiju akadēmija, Rēzekne, Latvija, 2024. 329 lpp.

**ENVIRONMENT. TECHNOLOGY. RESOURCES.** Proceedings of the 15<sup>th</sup> International Scientific and Practical Conference on June 27-28, 2024. *Volume IV*: Rezekne Academy of Technologies, Rezekne, Latvia, 2024. pp. 329.

Rekomendējusi publicēšanai Rēzeknes Tehnoloģiju akadēmijas Inženieru fakultātes Dome 2024. gada 29. maijā.  
*Recommended for publication by the Council of Faculty of Engineering of Rezekne Academy of Technologies on May, 29<sup>th</sup>, 2024.*

15.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 303 zinātniskie raksti. Konferences dalībnieki pārstāv 23 valstis.

**Šī konference un konferences materiālu krājums ir veltīti konferences "Vide. Tehnoloģija. Resursi" dibinātāja un konferences ilggadējā priekšsēdētāja profesora Dr.habil.geol. Gotfrīda Novika piemiņai.**

15.starptautiskās zinātniski praktiskās konferences "Vide. Tehnoloģija. Resursi" norises vieta ir "Vasil Levski" Nacionālā Militārā universitāte, Veliko Tarnovo, Bulgārija.

Proceedings of the 15th 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-based, on advances of international researchers. The proceedings comprise 303 scientific papers. Conference participants represent 23 countries.

***This conference and proceedings are dedicated to the conference "Environment. Technology. Resources" founder and long-time chairman of the conference, professor Dr.habil.geol. Gotfrīds Noviks memory.***

15th International Scientific and Practical Conference "Environment. Technology. Resources." hosted by "Vasil Levski" National Military University, Veliko Tarnovo, Bulgaria

<https://conferences.rta.lv/index.php/ETR/ETR2024>

Link to conference proceedings: <http://journals.rta.lv/index.php/ETR>



This journal is licenced under

[Creative Commons Attribution 4.0 International \(CC BY 4.0\) License](https://creativecommons.org/licenses/by/4.0/)

The author of the paper takes responsibility for the content of the paper.

Print ISSN 1691-5402

Online ISSN 2256-070X

Published by Rezekne Academy of Technologies, 2024

### ***Scientific Committee Chairman***

Dr.sc.ing. Edmunds Teirumnieks, Rezekne Academy of Technologies, 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 Technologies, Latvia

Dr.sc.ing. Artis Teilāns, Rezekne Academy of Technologies, Latvia

### ***Scientific Committee***

Dr.agr. Aleksandrs Adamovičs, Latvia University of Life Sciences and Technologies, Latvia

PhD Nikolaj Angelov, Technical University of Gabrovo, Bulgaria

Dr. agr. Lidia Antypova, Mykolayiv National Agrarian University, Ukraine

PhD Ekaterina Arabska, Higher School of Agribusiness and Regional Development, Bulgaria

PhD Iluta Arbidane, Rezekne Academy of Technologies, Latvia

PhD Daniel Berchev, "Vasil Levski" National Military University, Bulgaria

Dr. hab. Ing. Tadeusz Chrzan, Poltegor Institute, Poland

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

PhD Vanko Ganev, "Vasil Levski" National Military University, Bulgaria

Dr.sc.ing. Aleksandrs Gorbunovs, Riga Technical University, Latvia

Dr.sc.ing. Pēteris Grabusts, Rezekne Academy of Technologies, Latvia

PhD Grigor Grigorov, "Vasil Levski" National Military University, Bulgaria

PhD Mart Hovi, Estonian University of Life Sciences, Estonia

PhD Maria Ilcheva, Saint Cyril and Methodius University of Veliko Tarnovo, Bulgaria

Dr.paed. Ilmārs Kangro, Rezekne Academy of Technology, Latvia

Dr. paed. Janis Kapenieks, Riga Technical University, Latvia

PhD Tsanko Karadzhov, Technical University of Gabrovo, Bulgaria

PhD Aivars Kaupuzs, Rezekne Academy of Technologies, Latvia

PhD. Anna Khilya, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Spain

PhD Karīne Laganovska, Rezekne Academy of Technologies, Latvia

PhD Inga Ļašenko, Riga Technical University, Latvia

PhD Lazar Lazarov, "Vasil Levski" National Military University, Bulgaria

Dr.oec. Jeļena Lonska, Rezekne Academy of Technologies, Latvia

PhD Dilyan Markov, Georgi Rakovski Military Academy, Bulgaria

Brigadier General Ivan Malamov, "Vasil Levski" National Military University, Bulgaria

PhD Arturs Medveckis, Riga Technical University Liepaja Academy, Latvia

PhD Ziedonis Miklašēvičs, Rezekne Academy of Technologies, Latvia

Dr.sc.ing. Ivan Mitev, Technical University of Gabrovo, Bulgaria

PhD Cristian Emil Moldoveanu, Military Technical Academy "Ferdinand I", Romania

PhD Nikolay Nichev, Georgi Benkovski Higher Military Air School, Bulgaria

Dr.sc.ing. Neli Nikolova, Technical University of Gabrovo, Bulgaria

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

PhD Plamen Pavlov, School of Telecommunications and Posts, Bulgaria

Dr.sc.ing. Desislava Petrova, Technical University of Gabrovo, Bulgaria

Dr.agr. Liena Poiša, Rezekne Academy of Technologies, Latvia

Dr. agr. Valentīna Pole, IK Tava zeme, Latvia

PhD Todor Rachovski, Plovdiv University "Paisii Hilendarski", Bulgaria

Dr.sc.ing. Andris Skromulis, Rezekne Academy of Technologies, Latvia

PhD Krasimir Slavyanov, "Vasil Levski" National Military University, Bulgaria

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

PhD Aina Strode, Rezekne Academy of Technologies, Latvia

PhD Gunars Strods, Rezekne Academy of Technologies, Latvia  
Dr.sc.ing. Artis Teilāns, Rezekne Academy of Technologies, Latvia  
Dr.sc.ing. Edmunds Teirumnieks, Rezekne Academy of Technologies, Latvia  
PhD Ērika Teirumnieka, Rezekne Academy of Technologies, Latvia  
PhD Plamen Teodosiev, University of Library Studies and Information Technologies, Bulgaria  
Dr.-Ing. Josef Timmerberg, Jade University of Applied Sciences, Germany  
Dr.biol. Rasma Tretjakova, Rezekne Academy of Technologies, Latvia  
PhD Andra Ulme, Riga Technical University, Latvia  
PhD Nikolay Urummov, "Vasil Levski" National Military University, Bulgaria  
PhD Dragomir Vassilev, Technical University of Gabrovo, Bulgaria  
PhD Valentin Vassilev, South-West University "Neofit Rilski", Bulgaria  
PhD Emil Yankov, Rezekne Academy of Technologies, Latvia  
PhD Tsanka Zlateva-Petkova, Technical University of Gabrovo, Bulgaria  
PhD Anda Zvaigzne, Rezekne Academy of Technologies, 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  
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 Technologies, Latvia  
MA Georgi Hristov, "Vasil Levski" National Military University, Bulgaria  
Dr.sc.ing. Ēriks Kronbergs, Latvia University of Life Sciences and Technologies, Latvia  
Dr.sc.ing. Sergejs Kodors, Rezekne Academy of Technologies, Latvia  
Dr.sc.ing. Lyubomir Lazov, Rezekne Academy of Technologies, Latvia  
Dr.sc.ing. Andris Martinovs, Rezekne Academy of Technologies, Latvia  
PhD Rumen Marinov, Vasil Levski National Military University, Bulgaria  
PhD Magdalena Mitkova, Assen Zlatarov University Burgas, Bulgaria  
PhD Valyo Nikolov, Technical University of Sofia, Bulgaria  
PhD Nikolay Padarev, "Vasil Levski" National Military University, Bulgaria  
MA Svetoslav Pashunov, "Vasil Levski" National Military University, Bulgaria  
Dr.agr. Liena Poiša, Rezekne Academy of Technologies, Latvia  
Vilnis Rantins, Member of the Council of the Association of Mechanical Engineering and Metalworking Industries of Latvia, Latvia  
Dr.geol. Valdis Segliņš, University of Latvia, Latvia  
Dr.sc.ing. Andris Skromulis, Rezekne Academy of Technologies, Latvia  
Dr.biol. Artūrs Škute, Daugavpils University, Latvia  
Dr.sc.ing. Artis Teilāns, Rezekne Academy of Technologies, Latvia  
MA.sc.comp. Gundega Teilāne, Rezekne Academy of Technologies, Latvia  
PhD Ērika Teirumnieka, Rezekne Academy of Technologies, Latvia  
Dr.biol. Rasma Tretjakova, Rezekne Academy of Technologies, Latvia

### ***Reviewers***

Dr.agr. Aleksandrs Adamovičs, Latvia University of Life Sciences and Technologies, Latvia  
PhD Nikolaj Angelov, Technical University of Gabrovo, Bulgaria  
Dr. agr. Lidiia Antypova, Mykolayiv National Agrarian University, Ukraine  
PhD Ekaterina Arabska, Higher School of Agribusiness and Regional Development, Bulgaria  
PhD Iluta Arbidane, Rezekne Academy of Technologies, Latvia  
PhD Svetlana Asmuss, University of Latvia, Latvia

Dr.sc.ing. Anita Avišāne, Riga Technical University, Latvia  
PhD Stefan Bankov, The Ministry of Interior of Bulgaria, Bulgaria  
PhD Daniel Berchev, "Vasil Levski" National Military University, Bulgaria  
PhD Ansis Ataols Bērziņš, Riga Tehnical University, Latvia  
PhD Jānis Bičevskis, University of Latvia, Latvia  
PhD Rosen Bogdanov, "Vasil Levski" National Military University Sh, Bulgaria  
PhD Plamen Bogdanov, Library Studies and Information Technologies University, Bulgaria  
PhD Aija Brakovska, Daugavpils University, Latvia  
Dr. hab. Ing. Tadeusz Chrzan, Poltegor Institute, Poland  
PhD Maria Chunchukova, Agricultural University Plovdiv, Bulgaria  
PhD Dimitar Dichev, Technical University of Gabrovo, Bulgaria  
PhD Nikolay Dolchinkov, "Vasil Levski" National Military University, Bulgaria  
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  
Dr.sc.ing. Aleksandrs Gorbunovs, Riga Technical University, Latvia  
PhD Jānis Grabis, Riga Technical University, Latvia  
Dr.sc.ing. Pēteris Grabusts, Rezekne Academy of Technologies, Latvia  
PhD Grigor Grigorov, "Vasil Levski" National Military University, Bulgaria  
Dr. agr. Elvyra Gruzdevienė, Flax museum, the branch of Eriskiai Cultural Center of the Panevezys District, Lithuania  
PhD Mart Hovi, Estonian University of Life Sciences, Estonia  
PhD Iliayn Hutov, Defense Institute "Professor Tsvetan Lazarov", Bulgaria  
PhD Maria Ilcheva, Saint Cyril and Methodius University of Veliko Tarnovo, Bulgaria  
PhD Valery Ivanov, Defense Institute "Professor Tsvetan Lazarov", Bulgaria  
PhD Amit Joshi, BA school of banking and finance, Latvia  
Dr.sc.ing. Aivars Kaķītis, Latvia University of Life Sciences and Technologies, Latvia  
Dr.paed. Ilmārs Kangro, Rezekne Academy of Technology, Latvia  
Dr. paed. Janis Kapenieks, Riga Technical University, Latvia  
PhD Tsanko Karadzhev, Technical University of Gabrovo, Bulgaria  
PhD Aivars Kaupuzs, Rezekne Academy of Technologies, Latvia  
PhD. Anna Khilya, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Spain  
PhD Andrejs Koliškis, Riga Technical University, Latvia  
PhD Georgi Komitov, Agricultural University Plovdiv, Bulgaria  
Dr.sc.ing. Ēriks Kronbergs, Latvia University of Life Sciences and Technologies, Latvia  
PhD Karīne Laganovska, Rezekne Academy of Technologies, 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.oec. Jelena Lonska, Rezekne Academy of Technologies, Latvia  
Dr.sc.math. Maksims Marinaki, University of Latvia, Latvia  
PhD Georgi Marinov, Rakovski National Defence College, Bulgaria  
PhD Rumen Marinov, Vasil Levski National Military University, Bulgaria  
PhD Assen Marinov, "Georgi Benkovski" Bulgarian Air Force Academy, Bulgaria  
PhD Dilyan Markov, Georgi Rakovski Military Academy, Bulgaria  
PhD Arturs Medveckis, Riga Technical University Liepaja Academy, Latvia  
PhD Ziedonis Miklašēvičs, Rezekne Academy of Technologies, Latvia  
PhD Roussi Minev, Ruse University, Bulgaria  
PhD Nikolai Minkovski, University of Forestry, Bulgaria  
Dr.sc.ing. Ivan Mitev, Technical University of Gabrovo, Bulgaria  
PhD Linko Nikolov, "Vasil Levski" National Military University, Bulgaria  
Dr.sc.ing. Neli Nikolova, Technical University of Gabrovo, Bulgaria  
Dr.chem. Sergejs Osipovs, Daugavpils University, Latvia

PhD Nikolay Padarev, "Vasil Levski" National Military University, Bulgaria  
PhD Jana Paidere, Daugavpils University, Latvia  
PhD Hristian Panayotov, Technical University of Sofia, Bulgaria  
PhD Stanimir Parvanov, "Vasil Levski" National Military University, Bulgaria  
PhD Plamen Pavlov, School of Telecommunications and Posts, Bulgaria  
Dr.sc.ing. Jeļena Pečerska, Riga Technical University, Latvia  
PhD Penyo Penev, "Georgi Benkovski" Bulgarian Air Force Academy, Bulgaria  
Dr.sc.ing. Desislava Petrova, Technical University of Gabrovo, Bulgaria  
Dr.agr. Liena Poiša, Rezekne Academy of Technologies, Latvia  
Dr. agr. Valentīna Pole, IK Tava zeme, Latvia  
PhD Dimcho Pulov, Technical University of Gabrovo, Bulgaria  
Dr. agr. Gundega Putniece, Latvia University of Life Sciences and Technologies, Latvia  
PhD Todor Rachovski, Plovdiv University "Paisii Hilendarski", Bulgaria  
Dr.phys. Gita Rēvalde, Riga Technical University, Latvia  
PhD Jolanta Šadauskiene, Kaunas University of Technology, Lithuania  
Dr.sc.math. Felikss Sadirbajevs, Daugavpils University, Latvia  
PhD Andrejs Šiškins, Riga Technical University, Latvia  
Dr.sc.ing. Andris Skromulis, Rezekne Academy of Technologies, 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 Stoyko Stoykov, "Vasil Levski" National Military University, Bulgaria  
PhD Aina Strode, Rezekne Academy of Technologies, Latvia  
PhD Gunars Strods, Rezekne Academy of Technologies, Latvia  
Dr.sc.ing. Artis Teilāns, Rezekne Academy of Technologies, Latvia  
Dr.sc.ing. Edmunds Teirumnieks, Rezekne Academy of Technologies, Latvia  
PhD Plamen Teodosiev, University of Library Studies and Information Technologies, Bulgaria  
Dr.-Ing. Josef Timmerberg, Jade University of Applied Sciences, Germany  
Dr.biol. Rasma Tretjakova, Rezekne Academy of Technologies, Latvia  
PhD Andra Ulme, Riga Technical University, Latvia  
PhD Nikolay Urummov, "Vasil Levski" National Military University, Bulgaria  
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 Technologies, Latvia  
Dr.sc.ing. Imants Zarembo, Rezekne Academy of Technologies, Latvia  
PhD Tsanka Zlateva-Petkova, Technical University of Gabrovo, Bulgaria  
PhD Anda Zvaigzne, Rezekne Academy of Technologies, Latvia

### ***Secretariat Chairman***

PhD Ērika Teirumnieka, Rezekne Academy of Technologies, Latvia

### ***Secretariat Members***

Dr.agr. Liena Poiša, Rezekne Academy of Technologies, Latvia

MA.sc.comp. Gundega Teilāne, Rezekne Academy of Technologies, Latvia



**DEFENCE AND SECURITY  
TECHNOLOGIES**

# SATURS CONTENTS

## *Defence and security technologies*

<b>Olena Agapova, Giga Abuseridze, Andrii Svintsytskyi, Janis Grasis</b> BUILDING RESILIENCE OF UKRAINIAN UNIVERSITIES IN THE FACE OF MILITARY INTERVENTION: EXPLORING FORMS AND IMPLICATION	13
<b>Andon Andonov, Radoslav Chalakov</b> METHOD FOR KINETIC ARMOUR-PIERCING MUNITIONS EFFECTIVENESS ESTIMATION	19
<b>Andrii Andres, Nataliia Sorokolit, Andrii Mandiuk, Olha Rymar, Olena Khanikiants</b> THE IMPACT OF SPORTS ACTIVITIES ON THE PSYCHO-EMOTIONAL STATE OF CADETS IN HIGHER EDUCATION INSTITUTIONS DURING WARTIME	23
<b>Anelia Atipova</b> THE EUROPEAN TEMPORARY PROTECTION DIRECTIVE AND THE UKRAINIAN REFUGEE CRISIS	27
<b>Blagovest Bankov</b> ANALYSIS OF THE FORMATION OF CAVITATION CAVITY DURING THE MOVEMENT OF A MODIFIED BULLET OF 7.62X39 AMMUNITION IN A WATER ENVIRONMENT	32
<b>Blagovest Bankov</b> ANALYSIS OF THE INFLUENCE OF THE OGIVE RADIUS OF A 7.62X39 AMMUNITION BULLET ON THE CAVITATION CAVITY	37
<b>Ilze Bērziņa</b> THE IMPORTANCE OF DESIGNING OF INFORMATION SYSTEMS AND DATA EXCHANGE POSSIBILITIES TO CARRY OUT MULTIDISCIPLINARY COOPERATION TO PREVENT VIOLENCE AGAINST CHILDREN	41
<b>Jordan Deliversky</b> ILLEGAL MIGRATION PROCESSES MANAGEMENT IN THE LIGHT OF THE NEW EUROPEAN UNION PACT ON MIGRATION AND ASYLUM	45
<b>Todor Dimitrov</b> APPLYING ARTIFICIAL INTELLIGENCE FOR IMPROVING SITUATIONAL AWARENESS AND THREAT MONITORING AT SEA AS KEY FACTOR FOR SUCCESS IN NAVAL OPERATION	49
<b>Yana Dimitrova</b> ANALYTICAL MODEL FOR DETERMINING THE FRICTION FORCE AT THE CONTACT OF A METAL BODY WITH A COPPER CONTACT SURFACE	56
<b>Yana Dimitrova</b> EVALUATION OF WEAR MECHANISM OF SPECIAL PURPOSE MACHINE ELEMENTS	61
<b>Dilyana Dimitrova, Ivaylo Dimitrov</b> SECURITY ANALYSIS OF LIGHTWEIGHT CRYPTOGRAPHIC ALGORITHMS	65



<b>Radostin Dimov, Zhaneta Savova</b> ANTIVIRUS PERFORMANCE EVALUATION AGAINST POWERSHELL OBFUSCATED MALWARE	71
<b>Jelena Djubina</b> THE GENESIS OF THE CRIMINAL'S PERSONALITY IN THE DIGITAL AGE	79
<b>Nikolay Todorov Dolchinkov, Nikolay Bonev Nichev</b> GAMMA-BACKGROUND RADIATION CONTROL SYSTEMS AS A FACTOR OF BULGARIA'S NATIONAL SECURITY	83
<b>Petko Dimov, Georgi Marinov</b> HAZARDS POSED BY THE WAR IN UKRAINE: A STUDY OF POPULATION INFORMATION RISK AND MITIGATION EFFORTS	89
<b>Grigor Grigorov</b> MOTIVATION FOR CHOOSING AN OFFICER CAREER	95
<b>Grigor Grigorov</b> MODEL FOR RECRUITING SERVICEMEN IN THE ARMED FORCES	101
<b>Yordan Hristov, Ivan Minevski</b> ALGORITHM FOR DIAGNOSIS OF THE TANK WEAPON STABILIZATION SYSTEM “COMPLEX 2E28M” IN „TARGETING“ MODE	109
<b>Maria Ilcheva</b> GREEN AND SOCIAL INNOVATIONS IN PROVIDING EFFECTIVE PREVENTION AND SECURITY FOR ACTIVE AGEING	113
<b>Nikolay Iliev</b> INDICATORS OF MILITARY CAPABILITIES OF ENEMY SABOTAGE- RECONNAISSANCE GROUPS AND THEIR MODELLING	117
THE NUCLEAR FAMILY IN MODERN TERRORISM	121
<b>Galina Hristova Ivanova, Ivan Nikolaev Minevski</b> METHODOLOGY FOR TESTING PHYSICAL SAMPLES (MODELS) OF A CHEMICAL POWER SOURCE INTENDED FOR SINGLE USE IN DEFENCE INDUSTRY PRODUCTS	125
<b>Galina Hristova Ivanova</b> DEVELOPMENT OF A PROGRAM FOR CONDUCTING TESTS WITH PHYSICAL SAMPLES OF A DEFENCE INDUSTRY PRODUCT	131
<b>Amit Joshi, Aivars Spilbergs, Elina Miķelsone</b> AI-ENABLED DRONE AUTONOMOUS NAVIGATION AND DECISION MAKING FOR DEFENCE SECURITY	138
<b>Komil Kerimov, Zarina Azizova</b> ADAPTIVE MODEL FOR PROTECTION OF ELECTRONIC RESOURCES AGAINST INFORMATION SECURITY THREATS	144
<b>Kaloyan Kolev, Yordan Shterev</b> WIRELESS SECURITY ISSUES	150

<b>Krastyu Ivanov Krastev</b> THE CONTRIBUTION OF THE MILITARY SCHOOL TO THE BUILDING OF THE NATIONAL SECURITY SYSTEM OF BULGARIA IN THE PERIOD 1878-1885	<b>155</b>
<b>Krasimir Kalev, Lyubomir Manov</b> A PRELIMINARY STUDY OF PHOTON RADIATION ATTENUATION FROM BALLISTIC PROTECTION MATERIALS	<b>160</b>
<b>Rosen Lazarov</b> RESEARCH ON THE CHANGE IN BALLISTIC CHARACTERISTICS OF AMMUNITION WITH A MODIFIED PROJECTILE SHAPE DURING ITS MOVEMENT IN AN AIR ENVIRONMENT	<b>164</b>
<b>Rumen Marinov</b> CONTEMPORARY CHALLENGES TO THE PROTECTION OF THE COUNTRY'S SOVEREIGNTY	<b>168</b>
<b>Rumen Marinov</b> MODEL OF MANAGEMENT OF PROCESSES AND PHENOMENA'S IN THE MILITARY SECURITY SYSTEM	<b>173</b>
<b>Dilyan Markov</b> USE OF ARTILLERY FIRE SUPPORT ASSETS IN THE ATTRITION APPROACH IN THE RUSSIA-UKRAINE CONFLICT	<b>178</b>
<b>Tsveta Veselinova Monova</b> LEGAL FRAMEWORK OF THE EU POLICY IN THE FIELD OF DEFENCE SPACE TECHNOLOGY	<b>183</b>
<b>Maria Neikova</b> LEGAL APPROACH TO IMPLEMENTING SECURITY MEASURES FOR COMBATTING THREATS TO NATIONAL CRITICAL INFRASTRUCTURES	<b>190</b>
<b>Nikolay Iliyanov Padarev</b> APPLICATION OF SOFTWARE PLATFORMS TO ENHANCE EARLY WARNING AND DETECTION SYSTEM CAPABILITIES FOR NUCLEAR WEAPONS THREAT	<b>194</b>
<b>Jakub Pavlik, Tomas Rozsypal</b> EFFECT OF PRECIPITATION AND CONTAMINATION ORIGIN ON THE EFFICIENCY OF PINACOLYL ALCOHOL IDENTIFICATION IN CONCRETE DEBRIS	<b>199</b>
<b>Irena Peteva, Ivanka Pavlova, Daniela Pavlova</b> EFFECTIVENESS OF ELECTRONIC GOVERNANCE IN CRISIS MANAGEMENT	<b>206</b>
<b>Nikolay Petrov</b> COMPLEX OF ACTIVITIES SUPPORTING THE MANAGEMENT OF THE RADIO FREQUENCY SPECTRUM IN MILITARY OPERATIONS	<b>210</b>
<b>Ivo Radulov, Teodora Georgieva</b> A SCREENING METHOD FOR C2 EXPERT ASSESSMENT	<b>213</b>
<b>Ivo G. Radulov</b> MODELLING OF CAPABILITY-BASED DEFENCE PLANNING PROCESSES	<b>218</b>

<b>Normunds Rudzitis, Aldis Čeveris, Dana Drubiņa, Sandra Karkliņa-Admine</b> A RISK-BASED CUSTOMS CONTROL SYSTEM IN FREE ZONES	224
<b>Vladislavs Sardiko</b> ATTITUDES OF LATVIAN EXTERNAL BORDER CUSTOM OFFICERS TOWARDS WORK	232
<b>Zhaneta Savova, Rosen Bogdanov</b> SOME SPECIFIC FEATURES IN THE CONSTRUCTION OF P-ARY REED-SOLOMON CODES FOR AN ARBITRARY PRIME P	237
<b>Hristo Stanev, Stefan Hristozov</b> APPLICABILITY OF JARUS SORA TO STATE UAS OPERATIONS IN DISASTER RELIEF	244
<b>Vladimir Statev</b> DOES COMBAT DEPLOYMENT EXPERIENCE AFFECT THE COMMANDER'S DECISION-MAKING PROCESS?	251
<b>Veselka Stoyanova</b> RESEARCH OF THE CHARACTERISTICS OF A STEGANOGRAPHY ALGORITHM IN IMAGES WHEN USING DIFFERENT ALPHABET	255
<b>Iliya Stoychev, Iliyan Hutov</b> NIGHT VISION MONOCULAR - BASIC ELEMENTS AND DEVELOPMENT TRENDS	260
<b>Stoyko Stoykov</b> THE SYSTEM OF EDUCATION, TRAINING AND RESEARCH IN THE FIELD OF SECURITY - MANAGING CHANGE THROUGH EXPERIENCE AND KNOWLEDGE	269
<b>Plamen Penkov Teodosiev</b> TRENDS IN THE DEVELOPMENT OF MODERN INTERNATIONAL RELATIONS. THE NEW CHALLENGES FOR DIPLOMACY	275
<b>Nikolay Tsvyatkov</b> MISSION COMMAND AND THE CHALLENGES OF THE EARLY 21-ST CENTURY	282
<b>Nikolay Tenev Urummov</b> COMMAND AND CONTROL SYSTEM OF THE COUNTRY'S DEFENSE	287
<b>Nikolay Tenev Urummov</b> IMPROVING THE LEADERSHIP, COMMAND AND CONTROL SYSTEM OF THE COUNTRY'S DEFENSE	291
<b>Steliana Yordanova, Ralitsa Yotova, Stoyan Boyanov, Stoyan Garov</b> TERRORISM – A BARBARIC TOOL AND ITS DISPROPORTIONATE COUNTERACTION IN THE CONFLICT BETWEEN HAMAS AND ISRAEL	295
<b>Radoslav Yoshinov, Monka Kotseva, Anastas Madzharov, Neda Chehlarova</b> IMPLYING CYBERSECURITY SKILLS FOR PUBLIC ADMINISTRATION EMPLOYEES	300
<b>Ralitsa Yotova</b> CONCEPTUAL MODEL OF AN AUTOMATED SYSTEM FOR PROCESSING INFORMATION FROM OPEN SOURCES AND DETECTING INFORMATION DEVIATIONS	305
<b>Zarko Zdravkov, Anelia Atipova</b> METHODOLOGY FOR EVALUATION OF STRATEGIC DOCUMENTS	312

**Martin Zahariev**

THE APPLICABILITY OF THE EU DATA PROTECTION RULES IN THE AREA OF  
NATIONAL SECURITY IN THE REPUBLIC OF BULGARIA

**317**

**Ivan Malamov**

STUDY OF THE OPERATION, MAINTENANCE, AND REPAIR SYSTEM OF THE  
BULGARIAN ARMED FORCES

**322**

# *Building resilience of Ukrainian universities in the face of military intervention: exploring forms and implication*

**Olena Agapova**

*Rīga Stradiņš University  
Rīga, Latvia  
Scientific Research Center of  
Independent Forensic of the Ministry  
of Justice of Ukraine  
Kyiv, Ukraine  
agapova-lena-@ukr.net*

**Giga Abuseridze,**

*Caucasus University  
Tbilisi, Georgia  
[gabuseridze@cu.edu.ge](mailto:gabuseridze@cu.edu.ge)*

**Svintsytskyi Andrii**

*Scientific Research Center of  
Independent Forensic of the Ministry  
of Justice of Ukraine  
Kyiv, Ukraine  
e-mail: [info@srcif.com.ua](mailto:info@srcif.com.ua)*

**Janis Grasis**

*Rīga Stradiņš University  
Rīga, Latvia  
[Janis.Grasis@rsu.lv](mailto:Janis.Grasis@rsu.lv)*

**Abstract.** This article explores the concept of organizational resilience in higher education institutions, which can enable them to deal with unexpected events, recover from crises, and contribute to future success. Despite the growing academic interest in resilience, there is a lack of consensus on its definition and how it works, highlighting the need for additional knowledge on the capabilities and conditions that make up sustainability. The authors contribute to this field by conceptualizing resilience as a meta capacity and breaking it down into three stages: adaptation, transformation, and anticipation. They also identify core capabilities, including strategic vision, operational flexibility, and a supportive culture, that form organizational resilience.

Drawing on process research, the authors provide an overview of the relationship and interaction between the different stages of resilience, as well as the main prerequisites and driving forces. They also propose four tools based on an analysis of European normative-legal acts that can restore stability in crisis situations. This study advances understanding of the complex and built-in construct of organizational resilience and offers insights that can inform future empirical work in this area. The article underscores the significance of cultivating resilience capabilities in higher education institutions, particularly during times of turbulence and ambiguity, to guarantee their enduring.

**Keywords:** *university resilience, crisis situation, war, intervention, public administration*

## I. INTRODUCTION

The sustenance of global academic sustainability and scientific advancement hinges upon the resilience of higher education and research systems amidst crisis scenarios. Resilience emerges as a linchpin in safeguarding the viability of higher education against diverse contemporary challenges such as the COVID-19 pandemic, emergencies, and acts of terrorism. While European universities have demonstrated remarkable adaptability in challenging environments, their existence during wartime conditions remains precarious. Against the backdrop of a globalized world, the exigency to cultivate resilience has surged, accentuated by the profound repercussions of the COVID-19 pandemic and ongoing geopolitical tensions, exemplified by the Russian intervention in Ukraine [1].

As of the end of 2021, Ukraine's national resilience was characterized and described as a delicate mosaic with various gaps and sociopsychological and socio-political weaknesses, strengths, and other peculiarities [2]. The launch of the invasion into Ukraine provoked the most serious military conflict in Europe since 1945 [3].

The military intervention of the Russian Federation in Ukraine became the reaction catalyst for the operational organization of various aid in European countries [4]. The Ukrainian case showed that the recover resilience is difficult process and implemented due to international and national stakeholders.

*Print ISSN 1691-5402*

*Online ISSN 2256-070X*

<https://doi.org/10.17770/etr2024vol4.8243>

© 2024 Olena Agapova, Giga Abuseridze, Andrii Svintsytskyi, Janis Grasis.

*Published by Rezekne Academy of Technologies.*

*This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).*

Nevertheless, the process of resilience recover of the Ukrainian research and education area now is realizing in the military conditions. It should be note, that universities are unlikely return to the pre-war status quo, consequently the situation in Ukraine research and education area will change the common approaches of ensuring resilience in European research and education area, bring the new approach in the recover resilience matter.

Simultaneously, the unsatisfactory level of awareness of the representatives of universities, scientific institutions, and other stakeholders about the types, relevant facilities for adaptation and management in challenging environments can negatively impact on the sustainability and continuity of educational and scientific activities.

In the chapters below the authors scrutinize the landscape of organizational resilience within Ukrainian universities amidst military intervention, aiming to unveil strategies for bolstering their endurance and adaptability.

## II. MATERIALS AND METHODS

In their exploration of various methods for university operations during emergencies, particularly in military operations, the authors embark on a theoretical journey, shedding light on commonly known measures.

The methodology adopted by the authors involves an extensive review of existing literature, spanning scholarly books, scientific journals, and official legal documents and publications, including those from the European Union. This approach lays a solid foundation for a theoretical inquiry and contextual framework to delve into the process of bolstering resilience amidst the challenging landscape of the Russian invasion and intervention in Ukraine.

To comprehensively navigate the dynamics of resilience-building amid the Russian intervention, the authors employ a spectrum of established scientific techniques, each meticulously chosen to facilitate a nuanced understanding within the constraints of the invasion and intervention. These techniques include:

**Analytical Method:** This method serves as a powerful tool for dissecting complex concepts, theories, and empirical data related to resilience. By identifying underlying patterns and insights, the authors aim to better navigate the intricacies of the Russian intervention.

**Comparative Method:** Drawing comparisons between different cases, contexts, or practices allows the authors to elucidate commonalities, disparities, and trends, thereby enhancing their understanding amidst the Russian intervention.

**Methods of Interpreting Legal Norms:** Scrutinizing legal documents and publications provides invaluable insights into the legal frameworks influencing and guiding resilience initiatives within the higher education landscape post-intervention. This is crucial for understanding the regulatory context within which universities operate during such crises.

**Historical Method:** By tracing the evolution of resilience-building strategies over time, the authors gain a historical perspective on how higher education institutions

have adapted to challenges amidst the intervention. This historical context is essential for informing present-day strategies.

**Induction and Deduction Methods:** By employing both inductive and deductive reasoning, the authors can infer broader insights about resilience-building within the context of the Russian intervention based on specific instances and empirical evidence. This allows them to bridge theory with real-world observations.

By amalgamating these scientific techniques, the authors aim to establish a robust and systematic approach to comprehend the intricate process of fostering resilience amidst the challenges posed by the Russian intervention in Ukraine. This convergence of methods facilitates a comprehensive exploration of strategies, mechanisms, and adaptations of higher education institutions as they navigate the unique challenges arising from the intervention.

## III. RESULTS AND DISCUSSION

**Resilience Priority in EU and NATO: Strategic Compass 2022 and New NATO Strategic Concept Analysis.** From the authors' perspective, resilience emerges as a paramount priority for both the EU and NATO, as underscored in the Strategic Compass 2022 and the new NATO Strategic Concept. The Strategic Compass emphasizes the imperative to boost research, technology development, and innovation throughout the EU, reducing strategic dependencies in critical technologies and value chains for security and defense, as proposed by the European Commission [5]. This resonates with the authors' understanding of the importance of technological advancement and innovation in bolstering resilience in the face of contemporary security challenges.

Similarly, the new NATO Strategic Concept stresses the criticality of ensuring national and collective resilience to safeguard nations, societies, and shared values. The integration of technological innovation, climate change, human security, and the Women, Peace, and Security agenda underscores the cross-cutting importance of resilience [6]. The authors view this holistic approach to resilience as essential for addressing multifaceted security threats effectively.

The EU's comprehensive measures aimed at ensuring sustainability across various sectors, including higher education, demonstrate the relevance of resilience-building initiatives. Additionally, the alignment of resilience goals with the Sustainable Development Goals (SDGs) emphasizes the interconnectedness of sustainability and resilience efforts [7]. The authors believe that embedding resilience within broader sustainability frameworks is crucial for long-term effectiveness.

It would be wise to mentioned that, building resilience issues are also inseparable from the ensuring of European Research Area Policy Agenda [8]. Europe's strategy for international cooperation in a changing world (European Commission), Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 [9] establishing the Recovery and Resilience Facility (Official Journal of the European Union) [10], Council Resolution

on a strategic framework for European cooperation in education and training towards the European Education Area and beyond (2021-2030) 2021/C 66/01 [11], The United Nations Sustainable Development Goals [12]. Strategy for the development of higher education in Ukraine for the period 2021-2023 etc [13].

According to the provisions of Strategic Compass 2022, a more hostile security environment requires a significant step forward and increased capacity and readiness for action, strengthening resilience and ensuring solidarity and mutual assistance [5]. In this context, the strengthening of individual mutually beneficial partnerships, when there is a common commitment to an integrated approach to responding to conflicts and crises, contributes to the development of potential, resilience, and also meets the interests of the EU.

The Outcome Document of the Ukraine Recovery Conference URC2022 «Lugano Declaration» emphasises the recovery process has to contribute to accelerating, deepening, broadening and achieving Ukraine's reform efforts and resilience in line with Ukraine's European path [14].

In conclusion, this legislative framework underscores the pivotal role of ensuring the sustainability of universities in maintaining stable educational and research activities amidst the intervention. From the authors' standpoint, universities play a crucial role not only in disseminating knowledge but also in fostering resilience and contributing to societal stability and progress.

**Resilience Restoration in Ukrainian Universities: Strategies for Recovery and Development.** According to the authors, the restoration of resilience within the education and research sector entails the implementation of a range of measures aimed at progressively adapting higher education institutions to crisis situations. These measures are designed to facilitate the resumption of educational and research activities.

A unique practice to support the resilience of Ukrainian universities is the development of numerous programmes at different levels. The authors call them tools or forms of resilience restoration and consider them as a set of actions of specific actors aimed at restoring the educational and research activities of higher education institutions. Moreover, these forms of support exist both at the national and international levels and involve a wide range of stakeholders: public authorities, businesses, university community, private sector, etc.

Thus, the tools for restoring the resilience of Ukrainian universities in crisis situations are quite different and can be divided into 4 large groups: 1) financial support for universities; 2) support for scientists and students who were forced to leave Ukraine; 3) digital transformation of the Ukrainian education and science system; 4) deepening cooperation through the instrument of mentoring to restore active educational and research work in the war and post-war periods [15].

Let's take a closer look at financial support. Substantial global financial efforts will be needed to rebuild Ukrainian universities after the war. The EU is currently making a significant contribution to the revival of Ukrainian universities, but in the medium and long

term, not only financial but also human resources will be needed to fully restore them.

On 5 April 2023, the Government of Ukraine, members of the G7 Steering Committee and representatives of international financial institutions discussed during the second meeting of the Multi-Agency Donor Coordination Platform the best way to coordinate economic support for Ukraine's immediate financing needs and future efforts for Ukraine's economic recovery and reconstruction. The Government of Ukraine presented its budgetary needs for 2023, estimated at \$39.9 billion [16].

This budget includes estimates of expenditures for the social, production, infrastructure and cross-cutting sectors that require prompt financial assistance. In the social sector, education and science are singled out as a separate sector.

The document Ukraine Rapid Damage and Needs Assessment: February 2022 - February 2023 (RDNA2), jointly prepared by a World Bank team, the Government of Ukraine, European Union agencies and the United Nations, estimates that the war has caused at least US\$4.4 billion in damage to educational institutions across Ukraine. As of 24 February 2023, at least 2,772 educational facilities were partially damaged and 454 were destroyed, representing about 10 per cent of all educational facilities (at all levels of education) in Ukraine (World Bank, 2023). Educational institutions in eastern Ukraine are considered to be the most affected, with a damage rate of 64%. Thus, Ukraine's education sector has suffered at least US\$0.8 billion in losses [16].

In a crisis, financial management mechanisms are an objective necessity to ensure the sustainability, quality and continuity of higher education institutions and the proper functioning of the education system as a whole. Suspension of educational and research activities is unacceptable, as it is a matter of national and European security.

An equally important task is to restore the educational process and ensure the quality of educational services in a crisis. According to the National Recovery Plan of Ukraine, synchronisation with the European Union's education and research area is a strategic step to improve the quality of education and science. At the same time, the reconstruction and provision of safe access to education and quality assurance of the educational process has been identified as a national priority in the war and post-war periods [17]. It is important that Ukraine continues pre-war reforms aimed at improving the equity, sustainability and efficiency of education.

**Empowering Ukraine's Education and Science: Challenges and Pathways to Collaboration.** The implementation of key measures to restore the education and science sector necessarily includes support for scientists and students who were forced to leave Ukraine. We can confidently say that it was with the assistance of the EU that the promptest measures were taken to support Ukrainian scientists. In order to provide guarantees for displaced researchers, specialists and students from Ukraine, a number of regulatory and advisory acts were adopted, namely: Guidelines on fast-track recognition of

Ukrainian academic qualifications [18], Communication from the Commission on Guidance for access to the labour market, vocational education and training and adult learning of people fleeing Russia's war of aggression against Ukraine [19], EURYDICE report: Supporting refugee learners from Ukraine in higher education in Europe 2022 [20], Lifelong guidance policy for Ukrainian refugees in the EU etc [21].

At least 2 million children have left Ukraine, in addition to a significant number of educators and researchers, and many are expected to remain abroad in other countries in Europe, contributing to brain drain and future demographic challenges for the country.

Displaced researchers and specialists from Ukraine face a number of factors while abroad: unemployment, employment procedures in another country, confirmation of qualifications, transition to remote work, language requirements, lack of funding for research, and deterioration of psycho-emotional state.

The bright side is that we can note the existence of special platforms for researchers from Ukraine that offer participation in ongoing and innovative projects funded by the European Union. At the same time, special scholarship programmes for researchers from Ukraine have been launched.

The largest project is the launch of the European Commission's ERA4Ukraine portal "European Research Area for Ukraine" [22], a place to provide information and support services for Ukrainian researchers temporarily displaced from Ukraine. MSCA4Ukraine is a new special scholarship scheme to support displaced researchers from Ukraine. This support will allow displaced researchers to continue their work in academic and non-academic organisations in EU Member States and Horizon Europe Associated Countries, while maintaining links with the research and innovation communities in Ukraine [23].

Preserving Ukraine's scientific potential to stimulate growth and limit the brain drain is the main goal of such projects. In the long run, this will have a positive impact on internationalisation and accelerate the process of joining the European education and research sectors. In addition, this forced outflow of researchers will contribute to the development of university research bases, research centres with foreign universities, and academic mobility programmes.

The digital transformation of universities is a factor that also affects the sustainability of universities. Timely investment in the creation of an effective digital system of educational institutions will ensure readiness to respond to any crisis situations - emergency, military, hybrid, epidemiological, climate, etc. Innovations in the development of digital transformation of universities may include the introduction of data-driven decision-making, the use of technology to improve access to education, and the development of support programmes for students at risk.

When universities were forced to close their campuses and switch to remote learning due to the Russian invasion, those that had already embraced digital transformation were better equipped to adapt and continue their operations. In this context, the concept of force majeure,

which refers to unforeseeable circumstances beyond human control, has become increasingly relevant to universities. In order to adapt to force majeure situations, universities need to have a robust digital infrastructure in place. This includes everything from online learning platforms to communication tools and data analytics systems.

Here are some ways that universities can use digital transformation to adapt to force majeure:

**Online learning:** Universities can use digital tools to deliver online courses and lectures, allowing students to continue their studies remotely. This includes the use of video conferencing, online collaboration tools, and other e-learning platforms.

**Virtual campus tours:** Universities can create virtual campus tours using 360-degree cameras and other digital tools, allowing prospective students to explore the campus from afar.

**Remote research:** Universities can provide remote access to research materials and data, allowing researchers to continue their work from home.

**Digital communication:** Universities can use digital tools such as email, chat platforms, and social media to communicate with students, faculty, and staff, keeping them informed about important updates and changes.

**Data analytics:** Universities can use data analytics to track student performance, monitor enrolment trends, and predict future outcomes. This can help universities make informed decisions during times of crisis.

Overall, digital transformation is essential for universities that want to adapt to force majeure situations. By embracing digital tools and practices, universities can continue to deliver high-quality education and research, even in the face of unforeseeable circumstances.

The war has demonstrated the urgent need to use digital technologies in the education system, which allows access to education to remain uninterrupted. The need for a high level of digital capacity and professional training of academic and research staff has become a challenge for Ukraine. Therefore, the education and science system needs fundamental digital changes to keep pace with global trends and help each person successfully realise their potential.

Very illustrative in terms of restoring the sustainability of universities are measures to deepen cooperation through the instrument of mentoring with the help of the Twinning Project, developed specifically for the Ukrainian case. The UK-Ukraine Twinning Initiative project is an institution-to-institution collaboration model coordinated by Cormack Consultancy Group and the President's Fund of Ukraine for Education, Science, and Sports with the support of Universities UK International. The initiative allows universities around the world to support their Ukrainian counterparts in real, concrete ways. The main drive behind Twinning is to keep the integrity of the Ukrainian higher education system, prevent brain drain, and help universities in Ukraine to come out of the crisis with added resources, skills, and robust international experience. Twinning entails a long-



term commitment (a minimum of 5 years) between participating institutions to foster sustainable and mutually beneficial partnerships [24]. A total of 71 higher education institutions took part in the Twinning project.

As an example, we can cite the cooperation between the National Aerospace University "Kharkiv Aviation Institute" and the University of Bristol (UK). With the support of the Twinning Office, meetings were held with the leadership of the University of Bristol, a Memorandum of Cooperation was signed, English language courses were launched for KhAI employees, project activities were launched, and joint educational and scientific events were held.

## I. CONCLUSIONS

In general, resilience measures in education include many support tools that influence the ability of the education system to adapt to changing circumstances, equipping teachers and students with the necessary skills to adapt and overcome challenges, building the capacity of education professionals, and implementing evidence-based programmes and policies that promote resilience.

An academic institution with high foresight has a metaphorical toolkit at its disposal that can be used in the face of disruptive events that threaten academic continuity.

In order to minimize the impact of force majeure events on research, universities need to have robust contingency plans in place that include strategies for research continuity and support. In this article, we have explored some key strategies that universities can use to support research continuity in times of crisis.

Based on the results of the study, the authors identify the following main areas of sustainability:

**Communication and collaboration tools:** Communication and collaboration are critical to the success of research projects, but in times of crisis, it can be challenging to maintain regular contact with research teams. Universities can use digital communication tools such as video conferencing, chat platforms, and project management software to facilitate collaboration and ensure that research teams stay connected.

**Funding support:** During times of crisis, funding for research projects can be impacted due to budget cuts or delays. Universities can provide additional funding support for ongoing research projects, redirect funds to critical areas, and support grant applications that focus on addressing the challenges presented by the crisis.

**Alternative research approaches:** When access to physical resources is limited, researchers may need to explore alternative approaches to their research. Universities can support this by providing training and resources to help researchers adapt to new methods, technologies, and approaches.

**Mental health and wellness support:** Research can be a stressful and demanding activity, and the added pressure of a force majeure event can exacerbate these challenges. Universities can provide mental health and wellness support to researchers to help them manage stress and maintain their wellbeing during challenging times.

In conclusion, force majeure events can disrupt research activities, but with careful planning and preparation, universities can mitigate the impact and support research continuity. By leveraging digital technologies, providing funding and support, and prioritizing mental health and wellness, universities can ensure that research continues to thrive in the face of unexpected challenges.

According to the authors, higher education institutions in Ukraine are facing various challenges that call for the creation of a Center for Restoring the Resilience of Universities. The Center would serve as a platform for developing and implementing policies and strategies to enhance the resilience of universities. To achieve this, the authors provide several recommendations.

Firstly, the Center should be established with a multidisciplinary team of experts in fields such as education, psychology, management, and public policy. This will ensure that the Center has the necessary expertise to develop effective resilience strategies for universities.

Secondly, the Center should develop a framework for resilience that outlines the key components necessary for universities to build resilience. This includes the development of adaptive strategies, the identification of risk factors, and the promotion of a culture of resilience.

Thirdly, the Center should foster collaboration among universities, government agencies, and other stakeholders to promote a collective approach to building resilience. Collaboration will enable universities to share best practices and resources and to learn from each other's experiences.

Fourthly, the Center should provide training and resources to universities to help them develop and implement resilience strategies. This will ensure that universities have the necessary skills and knowledge to build their resilience and respond effectively to challenges.

Fifthly, the Center should conduct research to identify emerging threats and opportunities and to evaluate the effectiveness of resilience strategies. This will enable universities to stay up-to-date with the latest trends and best practices in building resilience.

Finally, the Center should advocate for policy change at the national level to promote the resilience of universities and to address structural challenges that impede their resilience. This will require engagement with policymakers and other stakeholders to promote the importance of building resilience in the higher education sector.

The authors believe that by implementing these recommendations, the Center for Restoring the Resilience of Universities in Ukraine can play a vital role in enhancing the resilience of universities and contributing to the overall development of the higher education sector in Ukraine.

## II. REFERENCES

- [1] G.Abuseridze, International trade in the context of the COVID-19 pandemic. In: Bari, M., Alaverdov, E. (eds.) *Impact of Infodemic on Organizational Performance*, pp. 217–230. IGI Global (2021). (in English). <https://doi.org/10.4018/978-1-7998-7164-4.ch013> Accessed 10.03.2024.
- [2] D.Teperik, I. Miroshkin, O.Iliuk, A. Apetyk, L. Snihur, G.Senkiv, D.Dubov, and O. Pokalchuk, (2021). *Resilient Ukraine - a delicate mosaic? Society, Media, Security, and Future Prospects*. Research report. Tallinn, Estonia: International Centre for Defence and Security, ISBN 978-9916-9699-3-9 (pdf), <https://icds.ee/en/resilient-ukraine-a-delicate-mosaic-society-media-security-and-future-prospects> Accessed 10.03.2024.
- [3] A.Kurapov, V. Pavlenko, A. Drozdov, V. Bezliudna, A. Reznik, and R. Isralowitz, (2022). *Toward an understanding of the Russian-Ukrainian war impact on university students and personnel*. *Journal of Loss and Trauma*, 1–8.
- [4] G.Abuseridze, O. Agapova, I. Paliani-Dittrich, J. Grasis, and E. Kavelidze, (2023). *Migration From Georgia and Ukraine in the Context of Russian Aggression*. In E. Alaverdov & M. Bari (Eds.), *Handbook of Research on the Regulation of the Modern Global Migration and Economic Crisis* (pp. 107-121). IGI Global. URL: <https://doi.org/10.4018/978-1-6684-6334-5.ch007> Accessed 10.03.2024.
- [5] *A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security* (2022). Approved by General Secretariat of the Council 7371/22 URL: <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf> 19.05.2023.
- [6] *NATO Strategic Compass* (2022). Adopted by the Heads of State and Government of the NATO Allies. URL: [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf) Accessed 10.03.2024.
- [7] *Transforming our world: the 2030 Agenda for Sustainable Development*. Resolution adopted by the General Assembly on 25 September 2015. Retrieved from: [https://www.un.org/ga/search/view\\_doc.asp?symbol=A/RES/70/1&Lang=E](https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E) Accessed 10.03.2024.
- [8] *European Research Area Policy Agenda* (2021). Luxembourg: Publications Office of the European Union. Retrieved from: [https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/our-digital-future/european-research-area\\_en](https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/our-digital-future/european-research-area_en) Accessed 10.03.2024.
- [9] *Europe's strategy for international cooperation in a changing world* (2021). European Commission, Brussels, COM(2021) 252 final/2. Retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2021:252:REV1&rid=2> Accessed 10.03.2024.
- [10] *Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility* (2021). Official Journal of the European Union. Retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0241&qid=1667997764795> Accessed 10.03.2024.
- [11] *Council Resolution on a strategic framework for European cooperation in education and training towards the European Education Area and beyond (2021-2030)* 2021/C 66/01 (2021). Official Journal of the European Union. Retrieved from: [https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32021G0226\(01\)](https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32021G0226(01)) Accessed 10.03.2024.
- [12] *The Sustainable Development Goals* (2023). Official UNDP Web-page. Retrieved from: <https://www.undp.org/sustainable-development-goals> Accessed 10.03.2024.
- [13] *On approval of the Strategy for the Development of Higher Education in Ukraine for 2022-2032* (2022). Order of the Cabinet of Ministers of Ukraine, Strategy 23.02.2022 No. 286-p. Retrieved from: <https://zakon.rada.gov.ua/laws/show/286-2022-%D1%80#Text> Accessed 10.03.2024.
- [14] *Outcome Document of the Ukraine Recovery Conference URC2022 “Lugano Declaration”* (2022). Retrieved from: [https://uploads-ssl.webflow.com/621f88db25fbf24758792dd8/62c68e41bd53305e8d214994\\_URC2022%20Lugano%20Declaration.pdf](https://uploads-ssl.webflow.com/621f88db25fbf24758792dd8/62c68e41bd53305e8d214994_URC2022%20Lugano%20Declaration.pdf) Accessed 10.03.2024.
- [15] *Multi-agency Donor Coordination Platform ramps up efforts to help Ukraine address priority recovery needs in 2023* (2023). Official European Commission Web-page. Retrieved from: [https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip\\_23\\_2102/IP\\_23\\_2102\\_EN.pdf](https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_23_2102/IP_23_2102_EN.pdf) Accessed 10.03.2024.
- [16] *Ukraine Rapid Damage and Needs Assessment: February 2022 - February 2023* (English). (2023) Washington, D.C. : World Bank Group. Retrieved from: <http://documents.worldbank.org/curated/en/099184503212328877/P1801740d1177f03c0ab180057556615497> Accessed 19.05.2023.
- [17] *National Recovery Plan of Ukraine* (2022). Adopted on the Ukraine Recovery Conference in Lugano. Retrieved from: [https://uploads-ssl.webflow.com/621f88db25fbf24758792dd8/62c166751fcf41105380a733\\_NRC%20Ukraine%27s%20Recovery%20Plan%20blueprint\\_ENG.pdf](https://uploads-ssl.webflow.com/621f88db25fbf24758792dd8/62c166751fcf41105380a733_NRC%20Ukraine%27s%20Recovery%20Plan%20blueprint_ENG.pdf) Accessed 10.03.2024.
- [18] *Guidelines on fast-track recognition of Ukrainian academic qualifications* (2022). Retrieved from: <https://education.ec.europa.eu/sites/default/files/2022-06/guidelines-fast-track-recognition-ukrainian-academic-qualifications.pdf> Accessed 10.03.2024.
- [19] *Ukraine: Commission presents guidance to help people fleeing war access jobs, training and adult learning* (2022). European Commission - Press release. Retrieved from: [https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip\\_22\\_3620/IP\\_22\\_3620\\_EN.pdf](https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_22_3620/IP_22_3620_EN.pdf) Accessed 10.03.2024.
- [20] *Supporting refugee learners from Ukraine in higher education in Europe* (2022). European Commission, European Education and Culture Executive Agency, Publications Office of the European Union. Retrieved from: <https://op.europa.eu/en/publication-detail/-/publication/3a49a873-0bc2-11ed-b11c-01aa75ed71a1/language-en/format-PDF/source-262591754#> Accessed 10.03.2024.
- [21] *Lifelong guidance policy for Ukrainian refugees in the EU* (2023). European Centre of the Development of Vocational Training. Retrieved from: [https://www.cedefop.europa.eu/files/8144\\_en.pdf](https://www.cedefop.europa.eu/files/8144_en.pdf) Accessed 10.03.2024.
- [22] *ERA4Ukraine* (2023). An official website of the European Union. Retrieved from: <https://euraxess.ec.europa.eu/ukraine> Accessed 10.03.2024.
- [23] *MSCA4Ukraine* (2023). An official website of the SAR Europe. Retrieved from: [https://sareurope.eu/msca4ukraine/?utm\\_source=flexmail&utm\\_medium=e-mail&utm\\_campaign=euanewsletter920221269euanewsletteroctober20221021t072200316z&utm\\_content=msca4ukraine+fellowship](https://sareurope.eu/msca4ukraine/?utm_source=flexmail&utm_medium=e-mail&utm_campaign=euanewsletter920221269euanewsletteroctober20221021t072200316z&utm_content=msca4ukraine+fellowship) Accessed 10.03.2024.
- [24] *The UK-Ukraine Twinning Initiative* (2023). An official website of the Twinning Ukraine. <https://www.twinningukraine.com/> Accessed 10.03.2024.

# Method for Kinetic Armour-Piercing Munitions Effectiveness Estimation

**Andon Andonov**  
Command and Staff Faculty  
Rakovski National Defence College  
Sofia, Bulgaria  
a.andonov@rndc.bg

**Radoslav Chalakov**  
Command and Staff Faculty  
Rakovski National Defence College  
Sofia, Bulgaria  
r.chalakov@rndc.bg

**Abstract.** This paper presents a mathematical model and a computational module for armour-piercing munition (APM) effectiveness estimation. The topicality of this research arises from the necessity to automate the weaponeering process as part of Phase 3 of the Joint Targeting Cycle. The main objective of the study is to analyse the penetrator's structural material and munition's geometric characteristics impact over the depth of penetration into homogeneous steel armour plate Class I, in accordance with MIL-DTL-46100E/2008 standard. Scientific methods analysis, math modelling, data collection, simulation and synthesis were used during the study. As a result, the following conclusions were made: 1) the armour-piercing munitions' effectiveness depends mainly on the ratio between penetrating rod's density and the armour density, but not on the hardness of their penetrating elements; 2) the proposed model is an approximate empirical technique for armor-piercing munition effectiveness estimation; 3) iteratively finding solutions for different input variables makes it possible to determine the input conditions necessary to realize the desired damage effect on a target; 4) the computational module could be applied to the weaponeering process as part of the Joint Targeting Cycle.

**Keywords:** *weaponeering, engagement, penetration.*

## I. INTRODUCTION

Joint targeting is a process to select and prioritize targets and determine proper means to engage them in accordance with the existing operational requirements and available capabilities [1]-[3]. It is a logical sequence of steps that supports decision making by linking operation objectives and effects to achieve them, with appropriate kinetic or non-kinetic means of engagement over prioritized targets. Therefore, a key part of the process is the weaponeering.

Weaponeering defines the type and quantity of weapons required to achieve desired effect on a given target, taking into account its vulnerability, munition's damage effect, reliability, environmental conditions and engagement accuracy [4].

To estimate a weapon capability to realize a desired hypothesis (degree) of damage, it is necessary to know its effectiveness and target vulnerability. These are based on the results of statistical analysis and simulations, outcome of which are values for munition's general and partial damage effect characteristics [5].

## II. MATERIALS AND METHODS

### A. Area of Research

Depending on their damage effect, kinetic weapons are classified into two groups [7]:

- contact munitions – inflict target damage in case of a direct hit (cumulative, armour-piercing, concrete-penetrating, etc.);
- remote munitions – damage the targets when their warheads detonate at a certain distance from it (fragmentation, blast, incendiary, etc.).

The study comprises analysis of the damage mechanism of penetrating armour-piercing munitions. It resulted in creation of a computational module for determining their penetrating effect, that can be used for weaponeering needs.

### B. Armour-piercing Munitions

Important feature of APMs (calibre and sub-calibre) is the ability to penetrate the target at the expense of their kinetic energy. They are widely used against heavy and light-armoured targets by penetrating their armour protection and subsequently defeating vulnerable components and crew located within. Ideally, an APM equipped with explosive should penetrate the armour and detonate afterwards, causing damage from the resulting fragments, shock wave, and incendiary effect. When a non-explosive APM is used, the defeat of the target is achieved by mechanical impact of the weapon's core and debris formed because of the armour destruction [7].

Print ISSN 1691-5402  
Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8193>

© 2024 Andon Andonov, Radoslav Chalakov. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

In that case, damaging element is a high hardness armour-piercing core made of ultra-high strength steel (UHSS), tungsten, Ni or Co added tungsten carbide, or depleted uranium. A key factor determining its effectiveness is the kinetic energy on impact, so the core should have low drag, relatively large mass compared to other munitions, and a high muzzle velocity in the range of 700-1785 m/s or more. Important trend in APM

development over the years is the increase of the working length and diameter ratio of the penetrator. The initial values of about 13:1 for the Russian/Soviet 3BM3 and 3BM6 gradually increased to 40:1 for the modern US M829A2 with a depleted uranium penetrator, where the impact energy reaches 35,800 [7]. Fig. 1 shows geometrical characteristics of an APM.

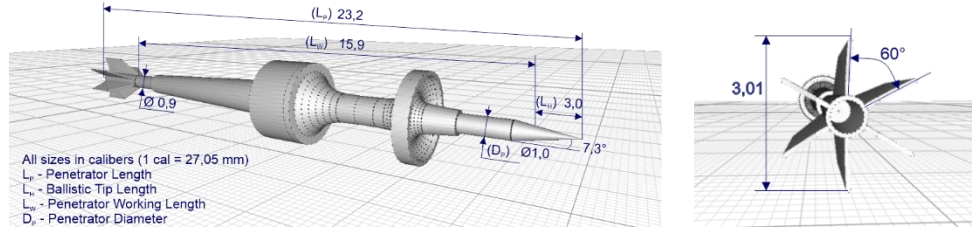


Fig. 1. APM geometric characteristics.

### C. Math Model

To study the APM penetration parameters the following assumptions have been made:

- the munition structure does not deform on impact;
- no loss of kinetic energy to deform the armour and destroy its fasteners;
- the conversion of kinetic energy to thermal energy is negligible;
- the munition longitudinal axis nutation, Coriolis force, Magnus effect and wind effect are ignored.

As moving along its trajectory, the APM speed constantly decreases due to the aerodynamic drag, which depends on the munition's middle cross section, angle of attack (in theory 0°) and drag coefficient. If suppose that its horizontal and vertical movement are independent, the initial velocity along both axes is determined as follows [4]:

$$v_{0x} = v_a \cos \gamma - v_e \sin \gamma \quad (1)$$

$$v_{0y} = v_a \sin \gamma + v_e \cos \gamma \quad (2)$$

$$v_p = 4000 \left( \frac{L_p}{d_a} \right)^{0,15} \sqrt{\left( \frac{D_p^3}{m_p} \right) \left[ \left( \frac{d_a}{D_p} \right) \left( \frac{1}{\cos \theta} \right)^{0,75} + e \left( \frac{d_a}{D_p} \left( \frac{1}{\cos \theta} \right)^{0,75} \right) - 1 \right]} \quad (4)$$

where:  $L_p$ -length [cm],  $D_p$ -diameter [cm] and  $m_p$ -mass of the penetrating rod, [g] ( $m_p = \frac{\pi}{4} D_p^2 L_p \rho_p$ );  $d_a$ -armour thickness along the surface normal [cm];  $\theta$ -impact angle relative to the surface normal [deg.];  $\rho_p$ - average density

where:  $v_{0x}$ -initial horizontal velocity [m/s];  $v_{0y}$ -initial vertical velocity [m/s];  $v_a$ -carrier velocity [m/s];  $v_e$ -release velocity [m/s];  $\gamma$ -trajectory inclination relative to the ground surface [deg].

In that way, the horizontal, vertical and total velocities on APM impact at a target, i.e., at a point with linear coordinates  $x$  and  $y$  would be:

$$V_i(x) = v_{0x} \cdot e^{-\left( \frac{c_d \cdot S_m \cdot \rho}{2G \sin \gamma} x \right)}$$

$$V_i(y) = v_{0y} \cdot e^{-\left( \frac{c_d \cdot S_m \cdot \rho}{2G \cos \gamma} y \right)} \quad (3)$$

$$V_i(\Sigma) = \sqrt{V_i(x)^2 + V_i(y)^2}$$

where:  $c_d$ -drag coefficient;  $S_m$ -area of the munition middle cross section [m<sup>2</sup>];  $\rho$ -air density [kg/m<sup>3</sup>];  $G$ -munition weight [kg].

To calculate the speed of impact required for penetration through homogeneous armour the Lambert's equation is used [8]:

of the penetrating rod [g/cm<sup>3</sup>].

Average density values of structural materials used for penetrating rods elaboration are given in Table 1 [9].

TABLE 1 STRUCTURAL MATERIALS AVERAGE DENSITY

$\rho_p$ , [g/cm <sup>3</sup> ]	Aluminum	UHSS	Depleted Uranium	Tungsten
	2,7 - 3	7,9 - 7,95	19,05	19,35

In order to estimate the penetration depth of APMs with UHSS, tungsten alloy or depleted uranium rod into an armoured plate, the Lantz-Odermatt equation could be used [7]:

$$L_{dp} = L_w \cdot k \cdot \frac{1}{\tanh(a_0 \cdot a_1 \cdot \eta)} \cdot (\cos \theta)^{a_2} \cdot \sqrt{\frac{\rho_p}{\rho_a}} \cdot e^{-\left( \frac{s^2}{v_p^2} \right)} \quad (5)$$

where:  $L_w$ -working length of the penetrator [mm];  $k$ -

coefficient dependent and  $a_0$ ,  $a_1$ ,  $a_2$ -coefficients independent of the rod material;  $\eta = L_w/D_p$ -length to diameter ratio of the rod;  $\tanh$ -hyperbolic tangent function;  $\rho_p$ -rod material density [kg/m<sup>3</sup>];  $\rho_a$ -armour material density [kg/m<sup>3</sup>].

In turn,  $L_w$  is determined mathematically for two ballistic tip shapes – cylindrical and conical:

$$L_w = L_p - \Delta L \quad (6)$$

$$\Delta L = L_h \left[ 1 - \frac{1}{3} \left( 1 + \frac{d_a}{D_p} + \left( \frac{d_a}{D_p} \right)^2 \right) \right] \quad (7)$$

where:  $L_h$ -length of the ballistic tip;  $\Delta L$ -relative length of the ballistic tip.

Depending on the penetrating rod material - tungsten alloy, depleted uranium ( $S_{dp/v}$ ), or UHSS ( $S_{hs}$ ), the value of  $s^2$  is calculated with the empirical relations shown:

$$S_{dp/v}^2 = \frac{(b_0 + b_1 \cdot HB_a) HB_p}{\rho_p} \quad (8)$$

$$S_{hs}^2 = \frac{b_0 \cdot HB_a^\alpha \cdot HB_p^\beta}{\rho_p} \quad (9)$$

where:  $b_0, b_1$ -coefficients independent of the rod material;  $HB_p$ -Brinell hardness number of the rod material;  $HB_a$ -Brinell hardness number of the armour structural material.

Values of the coefficients dependent and independent of the material properties used in equations (5), (8) and (9), are given in Table 2 [8].

TABLE 2 VALUES OF THE USED COEFFICIENTS

Coefficient	Material of the armour-piercing rod		
	UHSS	Depleted Uranium	Tungsten
k	1,104	0,825	0,994
$b_0$	9876	90,0	134,5
$b_1$	–	-0,0849	-0,148
$\alpha$	0,3598	–	–
$\beta$	-0,2342	–	–
$a_0$	0,283	0,283	0,283
$a_1$	0,0656	0,0656	0,0656
$a_2$	-0,224	-0,224	-0,224

After transformation, the Lanz-Odermatt equation acquires a simpler and more convenient for analytical modeling form:

$$L_{dp} = L_w \cdot f(\eta) \cdot (\cos \theta)^{a_2} \cdot \sqrt{\frac{\rho_p}{\rho_a}} \cdot e^{\left( \frac{-c \cdot \sigma_b}{\rho_p \cdot v_p^2} \right)} \quad (10)$$

where the function  $f(\eta)$  is determined empirically by the expression [7]:

$$f(\eta) = 1 + z_1 \frac{1}{\eta} \left( 1 - \tanh \left( \frac{\eta - 10}{z_2} \right) \right) \quad (11)$$

$$\eta = \frac{L_w}{D_p}, \quad (12)$$

the value of the variable  $c$  – by solving the polynomial:

$$c = 22,1 + 1,274 \cdot 10^{-2} \cdot \sigma_b - 9,47 \cdot 10^{-6} \cdot \sigma_b^2 \quad (13)$$

and the parameter  $\sigma_b$  is the tensile strength, i.e., tensile failure strength of the armor material, measured in [MPa]. For rolled homogeneous armor (RHA), the value of  $\sigma_b$  is about 800-1600 MPa.

An indirect approach to calculate the  $\sigma_b$  value for random structural material of the armor is to determine its Brinell hardness number  $HB_a$  and subsequently to use the dependences between the two parameters, valid when  $HB_a \leq 500$  [8], [10]:

$$\sigma_b = 3,4848(HB_a - 11,24) \quad (14)$$

$$HB_a = 0,287(\sigma_b - 39,1692) \quad (15)$$

Thus, in the range of  $\sigma_b = 800 \div 1600$  MPa,  $HB_a$  varies from 240 to 470.

The presented dependencies make it possible to evaluate the effectiveness of an APM against targets with different types of armour protection.

#### D. Computational Module

The proposed mathematical model is implemented by developing a computational module in Visual Basic® environment with the following characteristics:

*Purpose of the module:* Armor-piercing munition effectiveness calculation.

*Solved tasks:* 1) Predict the penetration depth in homogeneous armor in case of armor-piercing munition impact; 2) Estimate the relation between penetration depth and the penetrating element material or  $L_w/D_p$  ratio.

### III. RESULTS AND DISCUSSION

APM's effectiveness estimation in this study is based on two test scenarios.

The first scenario includes penetration depth calculation using APMs with constant geometric characteristics and different structural material of the penetrating element: 1) Steel AISI 4340; 2) Tungsten Alloy WNF-7129; 3) Depleted Uranium Alloy (U-Ti-Mo) Staballoy, in a Class I homogeneous armor plate, in accordance with MIL-DTL-46100E/2008 standard (UHTA Class I), at an impact angle  $\theta = 0^\circ$ , launched from different distances as in Table 3.

TABLE 3 MECHANICAL CHARACTERISTICS

Characteristic	AISI 4340	WNF-7129	Staballoy	UHTA Class I
$HB_p/HB_a$	341	271	185	330
$\rho_p/\rho_a$ [ $kg/m^3$ ]	7850	16850	19070	7980
$L_p$ , [mm]	350	350	350	-
$L_h$ , [mm]	45	45	45	-
$D_p$ , [mm]	30	30	30	-
$v_0$ , [m/s]	1500	1500	1500	-

The results from the first test scenario are shown in Fig. 2.

The second experiment is aimed to the penetration depth calculation of a WNF-7129 alloy piercing munition, for different length to diameter ratio of the rod ( $\eta = L_w/D_p = 10 \div 40$ ), with constant initial velocity  $v_0 = 1800$  m/s and angle of impact ( $\theta = 0^\circ$ ) in the same homogeneous armor plate (Class I, MIL-DTL-46100E/2008) (Fig. 3).

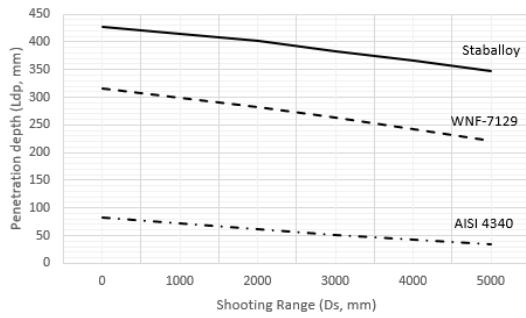


Fig. 2. Penetration depth for different structural materials of the piercing rod.

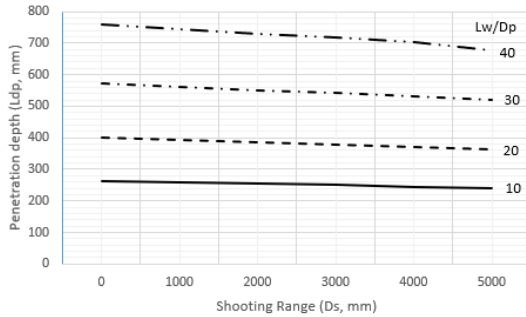


Fig. 3. Dependency between the penetration depth and the  $\eta = L_w/D_p$  ratio.

#### IV. CONCLUSIONS

The experimental results show that a key factor affecting the effectiveness of armor-piercing munitions is not the hardness of their penetrating elements, but the ratio between penetrating rod’s density and the armor density, when other conditions being equal. This determines the advantages of the contemporary munition made of tungsten alloy or depleted uranium (if don’t take into consideration the harmful influence of the latter on the environment and living organisms) compared to their steel counterparts.

In addition, the test scenarios highlight also another trend in this class of ammunition development – the continuous increase of  $\eta$  ratio. What is more, an increase in  $\eta$  by 10 units leads to an increase in the penetration depth by 25% ÷ 35%.

The proposed mathematical model and calculation module provide an approximate empirical approach to estimate the expected damage effect of an armor-piercing munition consisted of a kinetic penetrating element. Repeatedly finding solution to this direct problem with controlling the variables in the input data makes it possible to find a solution to the inverse problem as well, i.e., to determine the input conditions necessary to realize the desired damage effect on a target. Similar computational automation could be applied to the weaponeering process in Phase 3 of the Joint Targeting Cycle.

#### 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] Ministry of Defence of the Republic of Bulgaria, NP-3.3(A) Doktrina za vyzdushni operacii, Sofia, 2020.
- [2] Ministry of Defence of the Republic of Bulgaria, NP-3.9 Doktrina za syvmestno opredeljane i porazjavane na celite, Sofia, 2013.
- [3] K. Petkov, “Usyvyrshenstvane na planiraneto na operacii chrez standartiziran targeting model”, Dissertation, Rakovski National Defence College, Sofia, 2018.
- [4] M. R. Driels, “Weaponeering: An Introduction”. Third Edition, Volume 1, Virginia: AIAA Inc, 2019.
- [5] R. Dimitrov, “Bojno izpolzване na TA vuv vyzdushnite operacii”, Rakovski National Defence College, Sofia, 2019.
- [6] V. Zaporozhec, “Boevaja effektivnostj sredstv porazhenija i boepripasov”, Sankt-Peterburg: Baltijskij gosudarstvennyj tehnikeskij universitet, 2006.
- [7] W. S. Andrews, “Depleted Uranium on the Battlefield. Part 1 - Ballistic Considerations”, Canadian Military Journal, vol. 4, no. 2, Spring 2003, p.p. 41–46. [Online]. Available: <http://http://www.journal.forces.gc.ca/vo4/no1/research-recherch-eng.asp>. [Accessed: Jan. 25, 2024].
- [8] J. D. Walker, “Modern Impact and Penetration Mechanics”, Cambridge: Cambridge University Press, 2021.
- [9] The Engineering ToolBox. [Online]. Available: [https://www.engineeringtoolbox.com/density-solids-d\\_1265.html](https://www.engineeringtoolbox.com/density-solids-d_1265.html). [Accessed: Jan. 25, 2024].
- [10] American Society for Testing and Materials, “ASTM A370 Standard Test Methods and Definitions for Mechanical Testing of Steel Products, ed. 2022, ASTM International, ICS Code: 77.040.10”. [Online]. Available: <https://standards.iteh.ai/catalog/standards/astm/40dea6f1-3b28-42d9-900f-08bf0a1ae101/astm-a370-10>. [Accessed: Jan. 25, 2024].

# *The impact of sports activities on the psycho-emotional state of cadets in higher education institutions during wartime*

**Andriy Andres**

department of Physical Education  
Lviv Polytechnic National  
University)  
Lviv, Ukraine  
andres-a@ukr.net

**Nataliia Sorokolit**

department of theory and  
methodology of physical culture  
Lviv State University physical culture  
named after Ivan Bobersky  
Lviv, Ukraine  
sorokolit21@gmail.com

**Andrii Mandiuk**

department of theory and  
methodology of physical culture  
Lviv State University physical culture  
named after Ivan Bobersky  
Lviv, Ukraine  
a.b.mandyuk@gmail.com

**Olha Rymar**

department of theory and  
methodology of physical culture  
Lviv State University physical culture  
named after Ivan Bobersky  
Lviv, Ukraine  
okopiy@ukr.net

**Olena Khanikiants**

department of theory and  
methodology of physical culture  
Lviv State University physical culture  
named after Ivan Bobersky  
Lviv, Ukraine  
olena07lviv@gmail.com

**Abstract.** Military personnel with developed psychophysical qualities have a higher likelihood of success in their profession. The development of psychophysical preparedness can help maintain efficiency and health in extreme conditions. Today, there is a need to improve the psychophysical training of security and defense sector personnel in Ukraine. Engaging in sports can be one of the possible ways to enhance the psychophysical preparedness of the personnel in the security and defense sector of Ukraine.

However, differences in psychophysical indicators between cadet-athletes and cadets without sports experience in the conditions of full-scale war have not been determined. This complicates the process of forming recommendations for developing physical training programs for cadets.

Research methods used include theoretical analysis and summarization of scientific-methodical literature and internet data, sociological surveys (questionnaires), and methods of mathematical statistics.

Results have confirmed that sports activities have a positive impact on the psycho-emotional state of cadets: they shape a higher level of life satisfaction, personal stress resistance (without affecting situational anxiety); they increase the ability to control anger without affecting the ability to control emotions of depression and anxiety. Similar tendencies were observed for other psychophysical state indicators, which, however, did not statistically confirm, possibly explained by their heterogeneity.

**It can be recommended to engage in sports for the correction of the psychophysical state of cadets in higher education institutions during wartime conflicts.**

**Keywords:** anxiety, cadets, depression, emotional control, life satisfaction.

## I. INTRODUCTION

In the conditions of a full-scale war on the territory of Ukraine, there is an urgent need to improve the psychophysical training of the personnel in the security and defense sector of Ukraine. Military personnel with advanced psycho-physical qualities have a higher chance of success in their profession. The development of psycho-physical preparedness will help preserve efficiency and health in extreme conditions.

There is no universal solution on how best to prepare for effective actions in extreme conditions; however, a connection between the physical fitness of military personnel and their emotional control has been observed [1]. It is believed that sports activities can serve as an effective means of emotional regulation [2-8].

Available data in the specialized literature indicate that military personnel, cadets, and participants in combat often experience negative emotions [9-11] during peacetime or in the rehabilitation phase. However, there are not many scientific studies dedicated to highlighting

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8206>

© 2024 Andrii Andres, Nataliia Sorokolit, Andrii Mandiuk, Olha Rymar, Olena Khanikiants.

Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

the emotions experienced by military personnel in wartime conditions [12]. In stressful situations, the interaction of these indicators has not been studied. The lack of such data does not allow for the development of an effective training program for cadets. The purpose of the study: to determine what advantages exercise sports give to cadets of higher education institutions in the languages of full-scale war.

## II. MATERIALS AND METHODS

We conducted a survey of cadets (n=282) from higher education institutions. Depending on whether respondents continued to engage in sports regularly or ceased intensive training in their chosen sport, their data were divided into two groups.

The survey was conducted in the conditions of a full-scale war in the country (1.5 years after the Russian invasion). The surveyed cadets did not directly participate in combat; they continued their education in higher education institutions.

We distributed the questionnaire through Google Forms, determining indicators of the psycho-emotional state of cadets. The questionnaire included questions from standard techniques to assess the level of life

satisfaction (SWLS) [17], emotional control [18], anxiety [19].

The empirical data were described through key statistical indicators: mean (Mean), its error (SE), standard deviation (SD), median (Median), minimum (Lower), and maximum (Upper) values. To test the null hypothesis that the sample is derived from a normally distributed population, the Shapiro-Wilk Test was conducted. For comparing whether the mean values of psychodiagnostics results significantly differed between two samples, a one-way analysis of variance (One-Way ANOVA) was performed.

## III. RESULTS AND DISCUSSION

Previous engagement in sports positively impacted the psycho-emotional state of male and female cadets in the conditions of a full-scale war, as evidenced by a series of facts. For example, a higher level ( $p=0.05$ ) of subjective existential (non-situational) life satisfaction was observed in sports-oriented cadets ( $23.36 \pm 0.80$  points) compared to non-sports-oriented cadets ( $19.73 \pm 1.67$  points). The standard deviation indicated a large dispersion of values around the mean, suggesting significant variability in the subjective well-being indicators of cadets (Table 1).

TABLE 1 LEVEL OF WELL-BEING AMONG CADETS

Indexes	Sports*	95% Confidence Interval							Shapiro-Wilk	
		N	Mean	SE	Lower	Upper	Median	SD	W	p
Women	0	19	21.16	1.262	18.507	23.81	19	5.50	0.914	0.087
	1	45	22.44	0.692	21.051	23.84	23	4.64	0.936	0.016
Men	0	22	<b>19.73"</b>	1.674	16.246	23.21	20	7.85	0.972	0.755
	1	55	23.36	0.803	21.755	24.97	24	5.95	0.968	0.151

Notes: 1. \* – did not play sports, 1 – play sports;  
2. " - reliability of differences  $p=0.05$

Observing a similar trend in female cadets did not receive statistical confirmation. The life satisfaction scores we obtained were higher (better) than those of students from the University of Scotland ( $16.3 \pm 4.9$  points), Chinese students ( $16.1 \pm 4.4$  points), and Korean students ( $19.77 \pm 5.84$  points) [13]. However, our data were lower (worse) than the indicators typical for students in economically developed countries (measured in 1985-1993, ranging from 23.0 to 25.2) and military nurses ( $25.0 \pm 6.8$  points). Cadet indicators were similar to those of disabled students ( $20.8 \pm 8.4$  points and  $24.3 \pm 7.4$  points). Ukrainian female cadets assessed their well-being similarly to women who experienced physical, sexual, or emotional violence ( $20.7 \pm 7.4$  points).

The data summary revealed that both female and male cadets generally showed average levels of life satisfaction, typical for most people in economically developed countries. However, the dispersion of indicators was significant, indicating substantial individual differences. Cadets who continued to engage in sports had slightly higher indicators. Therefore, engaging in sports could be recommended for enhancing life satisfaction.

Due to the full-scale war, the level of reactive anxiety among cadets was high in all experimental groups. However, female cadets with sports experience had significantly ( $p < 0.05$ ) lower personal anxiety indicators ( $47.91 \pm 1.04$  points compared to  $49.84 \pm 2.39$  points) (Table 2).

Therefore, the data we obtained indicate that in the conditions of a full-scale war, the average anxiety level of cadets was high. However, the dispersion between maximum and minimum indicators was significant, suggesting substantial individual differences in the stress resistance level of cadets in both gender groups. Generalizing the obtained data allows us to suggest that engaging in sports contributes to reducing personal anxiety because indicators were somewhat lower for cadets who trained; in women, the tendency was statistically confirmed ( $p < 0.05$ ).

It can be assumed that the high anxiety levels in cadets were explained by professional stress during wartime combined with individual and personality traits. Similar but not as high anxiety indicators were observed among military personnel and combat participants.



TABLE 2 ANXIETY OF CADETS

Indexes	Sports *	95% Confidence Interval							Shapiro-Wilk	
		N	Mean	SE	Lower	Upper	Median	SD	W	p
<b>Women</b>										
Reactive anxiety	0	19	46.00	2.138	41.50	50.49	47	9.32	0.939	0.258
	1	45	47.22	0.804	45.60	48.84	47	5.39	0.973	0.359
Personal anxiety	0	19	49.84	2.393	44.81	54.87	51	10.43	0.761	<.001
	1	45	47.91"	1.037	45.82	50.00	49	6.96	0.848	<.001
<b>Men</b>										
Reactive anxiety	0	22	46.36	1.251	43.76	48.97	46	5.87	0.951	0.336
	1	55	46.98	0.791	45.39	48.57	48	5.86	0.978	0.410
Personal anxiety	0	22	46.45	1.606	43.11	49.79	46	7.53	0.956	0.414
	1	55	44.58	1.150	42.27	46.89	45	8.53	0.958	0.053

Notes: 1. \* – did not play sports, 1 – play sports;  
 2. " - reliability of differences p<0.05

According to experts [9], 30% of military personnel had a high level of personal anxiety, and 28% had high reactive anxiety. According to other data [14], 77% of combat participants had a high stress level, and 13% had a moderate level. It was found [15] that police cadets, on average, have a moderate level of professional anxiety, but senior cadets have a higher level of anxiety than first-year cadets. High prevalence of depressive symptoms was established [16] among military medical cadets. Therefore, according to our data, in wartime, the intensity of anxiety in cadets exceeded the indicators found in the scientific literature during peacetime military training.

The high level of anxiety inherent in cadets in peacetime is further intensified during wartime.

Anger control levels were significantly (p<0.05) lower in female cadets who did not engage in sports (14.53±1.17 points) than in those who continued training (17.24±0.52 points). Therefore, engaging in sports affects the ability of female cadets to control anger. However, depression and anxiety control indicators did not differ. This indicates that engaging in sports does not affect the ability to control these emotions in conditions of severe stress (Table 3).

TABLE 3 EMOTIONAL CONTROL OF CADETS

Indexes	Sports *	95% Confidence Interval							Shapiro-Wilk	
		N	Mean	SE	Lower	Upper	Median	SD	W	p
<b>Women</b>										
Anger control	0	19	14.53	1,176	12.056	17.00	14	5,12	0,926	0,145
	1	45	17.24"	0,520	16,196	18,29	17	3,49	0,972	0,346
Depression control	0	19	16.11	1,008	13,987	18,22	17	4,40	0,979	0,926
	1	45	16.80	0,567	15,657	17,94	17	3,81	0,981	0,656
Anxiety control	0	19	15.42	0,584	14,194	16,65	16	2,55	0,972	0,807
	1	45	15.51	0,420	14,665	16,36	16	2,82	0,966	0,207
<b>Men</b>										
Anger control	0	22	17.59	0,959	15,596	19,59	17,5	4,50	0,957	0,425
	1	55	17.38	0,553	16,274	18,49	18	4,10	0,982	0,569
Depression control	0	22	18.41	1,129	16,060	20,76	18,5	5,30	0,961	0,509
	1	55	16.87	0,615	15,640	18,11	18	4,56	0,970	0,192
Anxiety control	0	22	16.23	0,721	14,729	17,73	16,5	3,38	0,936	0,162
	1	55	15.49	0,500	14,488	16,49	16	3,71	0,973	0,239

Notes: 1. \* – did not play sports, 1 – play sports;  
 2. " - reliability of differences p<0.05

Generalizing the data on emotional control indicators among cadets showed that the study participants manage their emotions at an average level. However, significant dispersion between maximum and minimum results indicated heterogeneity in the emotional control levels of men and women. Engaging in sports affects the ability of female cadets to control anger, as evidenced by a significantly higher indicator (p<0.05).

#### IV. CONCLUSIONS

The study confirmed that engaging in sports has a positive impact on the psycho-emotional state of male and female cadets, leading to a higher level of personal life satisfaction (p=0.05) and personal stress resistance (p<0.05), without influencing situational anxiety. Sports experience enhances the ability to control anger (p<0.05) but does not affect the ability to control signs of depression and anxiety. Across a range of psychophysical state indicators, we observed similar trends that,

however, did not receive statistical confirmation, possibly due to their heterogeneity. This indicates significant individual differences in the stress resistance level of cadets in both gender groups. Engaging in sports is recommended for correcting the psychophysical state of cadets in higher education institutions during their professional activities.

## REFERENCES

- [1] S. K. Crowley, L. L. Wilkinson, L. T. Wigfall, A. M. Reynolds, et al. "Physical Fitness and Depressive Symptoms during Army Basic Combat Training", *Medicine & Science in Sports & Exercise*, vol. 47, no. 1, pp. 151–158, 2015. <https://doi.org/10.1249/MSS.0000000000000396>
- [2] V.V. Pichurin, "Psychological and psycho-physical training as a factor of personal anxiety at students" *Pedagogics, psychology, medical-biological problems of physical training and sports*, no. 3, pp. 46–52, 2015. [doi:10.15561/18189172.2015.0307](https://doi.org/10.15561/18189172.2015.0307)
- [3] V. Ziaee, S. Lotfian, H. Amini, M.A. Mansournia, A.H. Memari "Anger in Adolescent Boy Athletes: a Comparison among Judo, Karate, Swimming and Non Athletes". *Iranian Journal of Pediatrics*, vol. 22, pp. 9–14, 2012
- [4] G. Zieliński, A. Byś, M. Baszczowski, M. Ginszt, et al. „The influence of sport climbing on depression and anxiety levels – literature review”, *Journal of Education, Health and Sport*. vol. 8, no. 7, pp. 336–344, 2018.
- [5] K. Prontenko, G. Griban, V. Prontenko, F. Opanasiuk, et al., "Health improvement of cadets from higher military educational institutions during kettlebell lifting activities", *Journal of Physical Education and Sport*. 2018; vol. 18, no. 1, pp. 298–303.
- [6] I. M. Mazur, G. V. Bykova, S. M. Kozenko, Yu. M. Kornijchuk, ta in. "Dynamics of mental processes in cadets under the influence of physical training and sports ". V: *Naukovy'j chasopy's NPU imeni M. P. Dragomanova. Zb. nauk. pr.*, vol. 5, pp. 125, 2020. <https://doi.org/10.31392/NPUNC.SERIES15.2020.5%28125%29.18>
- [7] F. Szabo. "Do combat sports develop emotional intelligence?", *Kinesiology*, vol. 46, no. 1, pp.53–60, 2014.
- [8] S. Palevych, O. Poddubny, O. Tkachuk, Z. Tzymbaliuk, "Using mathematical criteria of evaluation for diagnostics results of cadets' training in affective sphere", *Health, Sport, Rehabilitation*, vol. 5, no. 1, pp. 96–106, 2019. <https://doi.org/10.34142/HSR.2019.05.01.11>
- [9] M.O. Yarmol'chuk, "Aggression and anxiety as determinants of the choice of coping strategies of military personnel during decompressionyi". *Social'na psy'xologiya; psy'xologiya social'noyi roboty'. Vcheni zapy'sky' TNU imeni V. I. Vernads'kogo. Seriya: Psy'xologiya*, vol. 32, no. 71, pp.109–114, 2021. <https://doi.org/10.32838/2709-3093/2021.2/19>
- [10] M.F. Crane, D. Boga, E. Karin, D.F. Gucciardi, F. Rapport, J. Callen, L. Sinclair. "Strengthening resilience in military officer cadets: A group-randomized controlled trial of coping and emotion regulatory self-reflection training". *Journal of Consulting and Clinical Psychology*, vol.87, no. 2, pp. 25–40, 2019. <https://doi.org/10.1037/ccp0000356>
- [11] D. Nasioudis, L. Palaiodimos, M. Dagiassis, et al. "Depression in military medicine cadets: a cross-sectional study", *Military Med Res.* vol. 2, no. 28, 2015. <https://doi.org/10.1186/s40779-015-0058-x>
- [12] I. Bodnar, A. Andres, V. Kryzhanovskiy, V. Shvets. "The influence of sports on emotional control in cadets of the national guard of ukraine at the beginning of the war". *Health Problems of Civilization*, vol. 17, no. 3, pp. 269-276, 2023. <https://doi.org/10.5114/hpc.2023.128805>
- [13] E. Diener. "Assessing Well-Being: Review of the Satisfaction With Life Scale. The Collected Works of Ed Diener", *Social Indicators Research Series 39*, [https://doi.org/10.1007/978-90-481-2354-4\\_5](https://doi.org/10.1007/978-90-481-2354-4_5)
- [14] N. Krushyn'ska, I. Kogut, "The influence of jogging on the stress level of combatants". *Theory and methodology of physical education and sports*. no. 4, pp. 37–41. 2022.
- [15] G. Uludağ, H. Taşdöven, M. Dönmez, "Polis Adaylarının Mesleki Kaygı Düzeylerinin Çeşitli Değişkenler Açısından İncelenmesi", *Current Perspectives in Social Sciences*, vol. 18, no. 2, pp. 75–94, 2014.
- [16] D. Nasioudis, L. Palaiodimos, M. Dagiassis, et al. "Depression in military medicine cadets: a cross-sectional study", *Military Med Res.*, vol. 2, no. 2, 2015. <https://doi.org/10.1186/s40779-015-0058-x>
- [17] E. Diener, R. Emmons, R. Larsen, S. Griffin. "The Satisfaction With Life Scale". *J Pers Assess.* Feb; vol. 49, no. 1, pp.71-5. 1985. doi: 10.1207/s15327752jpa4901\_13.
- [18] M. Watson, S. Greer. "Development of a questionnaire measure of emotional control". *J Psychosom Res.*; vol. 27 no. 4, pp. 299-305. 1983. doi: 10.1016/0022-3999(83)90052-1.
- [19] C. Spielberger, S. Sydeman. "State-Trait Anxiety Inventory and State-Trait Anger Expression Inventory". In Maruish, Mark Edward (ed.). *The use of psychological testing for treatment planning and outcome assessment*. Hillsdale, NJ: Lawrence Erlbaum Associates. pp. 292–321. 1994.

# The European Temporary Protection Directive And The Ukrainian Refugee Crisis

Anelia Atipova

The Defense Advanced Research  
Institute (DARI)  
National Defense College "G. S.  
Rakovski"  
Sofia, Bulgaria  
[a.atipova@rndc.bg](mailto:a.atipova@rndc.bg)

**Abstract.** The military conflict in Ukraine since the end of February 2022 has caused an unprecedented intra-European refugee crisis. More than 6 million Ukrainians left the country, and another 8 million were internally displaced. The policy of solidarity with the Ukrainian state faced the EU in exceptional circumstances and required a revision of the existing legislation in the field of international protection. The report offers a comparative analysis of the transposition practices of the Council Directive 2001/55/EC on minimum standards for the granting of temporary protection, activated for the first time since its adoption. The legislations of sixteen countries that have become the main receivers of the refugee flow have been examined, one of which is the Republic of Bulgaria.

**Keywords:** military conflict; refugee crisis; Temporary protection directive; Ukraine.

## INTRODUCTION

The military conflict in Ukraine since the end of February 2022 has faced Europe with a serious refugee crisis. 3.5 million people left the country in the first months after the bloodshed, seeking international protection in the EU [1]. In March 2023, their number increased to 3,888,345 million people [2], and in November of the same year, it was already 4.2 million people [3].

The massive influx of Ukrainians falling under two European [4], [5], [6] and one international [7] regulation, the lack of clarity about the outcome of the war and the exclusivity of the mechanisms for granting temporary protection in the EU complicate the case considerably.

The main problems arise when transposing Council Directive 2001/55/EC into national legislation. EU member states should develop their own normative instruments regulating the reception of mass refugee flows and their consequences.

## I. MATERIALS AND METHODS

The report uses the generally accepted methods of content analysis, criterion and statistical analysis and teleological legal analysis to summarize the results and trends in the implementation of the European directive framework for the regulation of mass influxes of refugees, through its transposition into national legislations.

The normative framework of the EU in the subject area, as well as the legislation of 16 member states, which experienced the most significant part of the refugee pressure, were examined.

In the analysis of the documents, the presumption was respected that the regime of temporary protection is not prejudicial to the recognition of refugee status (Article 3 of Directive 2001/55/EC) and does not cancel or replace the regulations for the granting of such status.

Official open sources, normative documents and statistical data of Eurostat and UNHCR were used.

## II. RESULTS AND DISCUSSIONS

### A. Dynamics of the Ukrainian refugee flow to the EU (2022-2024)

The dynamics of migration processes is determined by two categories of factors - pull factors and push factors. They vary with the mixed immigration flows consisting of refugees and illegal (economic) immigrants, as traditionally settled in the EU countries.

In a situation of military and/or humanitarian crisis, the social and economic pull factors do not disappear.

They are supplemented with other factors, with a higher degree of priority, such as the geographical proximity of the first safe country, the logistical possibilities for movement, the presence of an established diaspora (in this

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8219>

© 2024 Anelia Atipova. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

case, Ukrainian), the refugee-immigration policy of the host country, etc.

Geographically closest to Ukraine are the EU countries - Romania, Poland, Hungary, Slovakia, as well as Moldova and Belarus, the latter of which has diametrically opposed European policy regarding the conflict and the refugee crisis, as a result of it.

The geographical proximity does not fully correspond to the presence of Ukrainian citizens on the territory of the EU, before the conflict. According to Eurostat data, the largest Ukrainian diasporas are in Poland (651,221), Italy (230,360), the Czech Republic (193,547), Spain (97,442), Germany (83,043), Hungary (63,175), and Slovakia (54,138) [8] .

The number of asylum seekers in 2022 [9], 2023 [10] and 2024 [11], [12] , compared to the number of Ukrainians settled in the EU, also shows a discrepancy in the expectations for the choice of the first safe country, assumed by geographical proximity (Table 1).

TABLE I NUMBER OF UKRAINIAN CITIZENS IN EU COUNTRIES FOR THE PERIOD 2021-2024

Country	2021	2022	2023	2024
Bulgaria	9149	30505	166535	67770
Croatia	2405	240	22485	24355
Czech R.	193547	244650	357960	381400
Greece	20690	0	27365	26675
France	18610	26015	64775	65175
Germany	83043	700347	1194900	1235960
Hungary	63175	0	33060	65585
Italy	230360	0	161220	168840
Latvia	9087	12840	43035	43565
Lithuania	32884	3155	72810	52670
Poland	651221	675085	958655	955110
Portugal	27195	23930	57230	58490
Romania	2260	1980	140585	78745
Slovakia	54138	58750	109530	115875
Spain	97442	32445	187205	192405
Sweden	5768	17850	41915	42040

The countries with the largest Ukrainian diaspora also have the largest growth in persons seeking international protection (Table 1). From Graph 1, it is evident that the refugee pressure is the lowest in 2022, gradually increasing and reaching its peak in February 2024. The most affected countries are Germany, Poland, Czech Republic and Spain, while in Bulgaria, Italy, Lithuania and Romania, it is weakening.

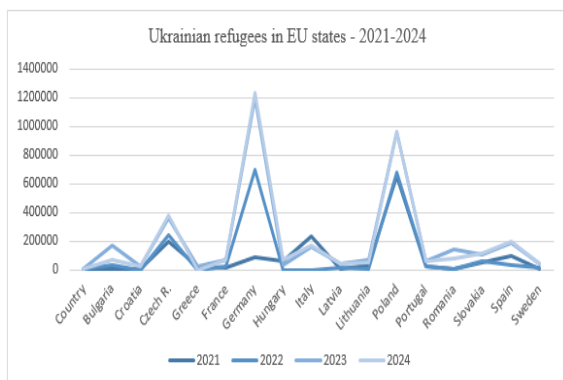


Fig.1. Ukrainian refugees in EU – 2021 – 2024

This clearly outlines the profile of the first group of countries as permanent settlement countries and the second group of countries as transit countries. The countries of the first group have a higher level of economic and social development and access to the labor market, which is crucial for accommodating the refugee contingent. However, the listed 16 countries bear the overwhelming burden of the refugee pressure from Ukraine and the responsibility for its management for a period defined in the European and national legislation.

*B. Overview of the regular basis for the grant of temporary protection in the EU*

*a) Directive 2001/55/EO*

The provision of temporary protection in case of a mass influx of displaced persons into the territory of the EU is regulated in Council Directive 2001/55/EC (TPD), adopted in 2001. It sets minimum standards in the subject area, with the aim of evenly distributing the responsibilities between Member States.

According to its provisions, this type of protection should be for a limited period of time and based on the principles of subsidiarity, proportionality and non-discrimination. In Art. 5 it is stated that "the existence of a mass entry of displaced persons is certified by a decision of the Council". On March 4, 2022, Implementing Decision (EU) 2022/382 [13] was adopted, and at the end of the same month operational guidelines for its implementation [14] came into force.

The main mechanisms for the management of mass refugee flows, which the Directive introduces, are the following:

1. Registration of people seeking temporary protection (art. 10, art. 17).
2. Mechanisms for termination of temporary protection and return of a beneficiary (Article 11).
3. Access to the labor market and social benefits (Article 12, Article 13, Paragraph 2).
4. Housing (Article 13, Paragraph 1).
5. Medical and psychological insurance (Article 14).
6. Access to education (Art. 14).
7. Right to family reunification, respecting the interests of the child (Article 15, Paragraph 4 and Paragraph 5).
8. Information exchange and access to information (Art. 26, Art. 27).

In addition, member states must develop mechanisms to differentiate immigration flows and exclude persons from access to international protection (item 22, art. 28), work with vulnerable groups (art. 16, art. 23) and mechanisms for return.

According to Art. 32, para. 1, when transposing Directive 2001/55/EC of the Council, when introducing the specified measures into national legislation, they must contain a reference to the Directive, in a manner adopted by the state.

*b) Implementing Decision (EU) 2022/382*

Implementing Decision (EU) 2022/382 specifies the refugee quota, according to the legal formulation of item 22 of Directive 2001/55/EC, for determining a criterion "for excluding certain persons from the circle of those who are granted temporary protection in a case of mass entry of displaced persons" and reduces the action to only persons coming from the territory of Ukraine.

Item 6 of the Decision assumes that, given their right to free visa-free entry and stay for 90 days within 180 days, on the territory of the EU, "it is expected that half of the Ukrainians coming to the Union [...] will join to family members or to seek employment in the Union, and the other half to seek international protection".

The decision also states that, in accordance with the Directive, "Member States may extend the scope of temporary protection to stateless persons or third-country nationals legally residing in Ukraine who cannot return permanently and under safe conditions to their country or region of origin" (item 13).

*c) Issues arising from the framework for granting temporary protection in the EU*

The status of a beneficiary of temporary protection cannot be combined with that of a person applying for refugee status while the application is being processed. Thus, temporary protection is the only effective tool to prevent mass applications for refugee status from overwhelming national asylum systems and leaving states unable to manage the process.

However, there are several significant problems that the transposition of Directive 2001/55/EC into national legislation may cause:

1. Since 2017, Ukrainians enjoy the right to freely enter the territory of all EU countries, therefore they can choose in which country to receive temporary protection. Despite the intention of this assumption to spread the burden of refugee pressure evenly, countries with higher economic growth are more burdened, as can be seen from the statistics in Table 1.

2. To date, temporary protection for those coming from the territory of Ukraine has been extended twice, for a period of 1 year each. Its final term of operation is March 4, 2025. [15] This creates preconditions for burdening the social system, at the expense of the asylum system of the member states, since the potential contribution of Ukrainian refugees to the labor market in the receiving countries is uncertain, due to difficulties in the integration process [16], although the regulatory framework allows inclusion in the labor market.

3. In 2025, a new travel authorization for Ukrainian citizens (Electronic Travel Authorization System, ETIAS) [17] will enter into force, according to which each person will receive individual access to EU member states, after a thorough check in European bases -security data (eu-LISA, the Schengen Information System (SIS), INTERPOL, EURODAC, EUROPOL and the Visa Information System (VIS)). The provisions do not apply to beneficiaries of temporary protection at present, but severely limit the ability to prorate the refugee burden in future movements.

The minimum standards should be introduced and further developed by transposing Directive 2001/55/EC into the national legislation of the member states.

*C. Analysis of the national legislation for the transposition of Directive 2001/55/EC*

The transposition of Directive 2001/55/EC into the national legislation of 16 countries, which received the largest part of the refugee pressure from Ukraine, was analyzed. The analysis was performed according to synthesized 8 criteria, and the results are summarized in Table 2.

TABLE II LEVEL OF TRANSPOSITION OF DIRECTIVE 2001/55/EC INTO THE NATIONAL LEGISLATION OF 16 EU COUNTRIES

Country	Criteria			
	Mechanism for excluding from TMD	Registration of people	Access to labour market	Access to education
Bulgaria	Yes	Partly	Yes	Yes
Croatia	Yes	Yes	Yes	Yes
Czech R.	Yes	Partly	Yes	Yes
France	Yes	Partly	Yes	Yes
Germany	Yes	Yes	Yes	Yes
Greece	Yes	Partly	Yes	Yes
Hungary	Yes	Partly	No	Yes
Italy	Yes	Yes	Yes	Yes
Latvia	Yes	Partly	Yes	Yes
Lithuania	Yes	Yes	Yes	Yes
Poland	Yes	Partly	Yes	Yes
Portugal	Yes	Yes	Yes	Yes
Romania	Yes	Yes	Yes	Yes
Slovakia	Yes	Partly	Yes	Yes
Spain	Yes	Yes	Yes	Yes
Sweden	Yes	Yes	Yes	Yes
Country	Criteria			
	Access to health care	Access to social housing	Vulnerable groups protection	Provision of information
Bulgaria	Yes	Yes	Yes	Yes
Croatia	Yes	Yes	Yes	Yes
Czech R.	Yes	Yes	Yes	Yes
France	Yes	Yes	Yes	Yes
Germany	Yes	Yes	Yes	Yes
Greece	Yes	No	Yes	Yes
Hungary	Yes	Yes	Yes	Yes
Italy	Yes	Yes	Yes	Yes
Latvia	Yes	Yes	Yes	Yes
Lithuania	Yes	Yes	Yes	Yes
Poland	Yes	Yes	Yes	Yes
Portugal	Yes	Yes	Yes	Yes
Romania	Yes	Yes	Yes	Yes
Slovakia	Yes	No	Yes	Yes
Spain	Yes	Yes	Yes	Yes
Sweden	Yes	Yes	Yes	Yes

The analysis shows that 7 of the 16 countries transpose Council Directive 2001/55/EC into their existing legislation and by Decision of the Council of Ministers or another responsible institution (Bulgaria, Hungary, Italy, Portugal, Romania, Spain and Sweden) , and 9 adopt special normative acts for Ukraine [18] (Croatia, Czech

Republic, France, Germany, Greece, Latvia, Lithuania, Poland and Slovakia).

Countries with changes to existing legal norms create legal resilience and build capacity to deal with future mass refugee flows. These are also the countries with the greatest refugee-immigration experience.

A total of 14 countries benefit from what is specified in Art. 7, para. 1 of Directive 2001/55/EC right to expand the categories of persons, beneficiaries of temporary protection. The cases of Spain, Germany and Lithuania stand out, where, in addition to Ukrainian citizens and citizens of third countries residing in Ukraine, there are also illegally residing Ukrainians and Ukrainians legally residing in other EU countries. Latvia and Slovakia do not expand the categories for accepting refugees from Ukraine.

The national practices of 8 countries differ on the fingerprinting procedure at registration. Hungary stands out for not giving beneficiaries of international protection access to the labor market. Slovakia and Greece do not provide accommodation.

A total of 13 countries bind the granting of international protection to the date of 24 February 2022, as follows:

1. Ukrainian citizens and third-country nationals residing in Ukraine or in an EU accession country before February 24, 2022 – 5 countries (Sweden, Slovakia, Italy, Czech Republic and Bulgaria).

2. Ukrainian citizens and citizens of third countries who left Ukraine before February 24, 2022 – 3 countries (Lithuania, Germany and Croatia).

3. Ukrainian citizens and citizens of third countries who left Ukraine after February 24, 2022 – 4 countries (Poland, Hungary, Greece and France).

4. Ukrainian citizens and citizens of third countries who left Ukraine before February 24, 2022 – 3 countries (Lithuania, Germany and Croatia).

5. Ukrainian citizens and citizens of third countries who left Ukraine before or after February 24, 2022 – 1 country (Romania).

Portugal, Spain and Latvia do not bind the granting of temporary protection to displaced persons from the territory of Ukraine, with departure or residence before or after February 24, 2022.

Tying temporary protection status to a specific date means that all refugee flows out of the country after that date will be internally displaced, flow into illegal immigration flows or claim refugee status. A part of them will be redirected to the countries that do not bind their refugee policy towards Ukraine with time specifics and thus, they will violate the proportionality of the reception.

On the other hand, the option of visa-free travel and stay in the EU for a period of 90 days becomes a highly selective practice due to the entry into force of ETIAS from 2025.

The differentiation of the refugee-immigration flows from the country to the EU and the redistribution of the administrative capacity of the asylum systems to manage them are not a permanent solution to the problem. Steps are needed towards sustainable integration of Ukrainians in EU member states.

This is particularly relevant in the countries with the largest influx of refugees from Ukraine, presupposed by the factors of diaspora presence, socio-economic level and refugee policy, including the transposition of Directive 2002/55/EC into their national legislations.

#### CONCLUSION

The analysis of the national practices of 16 EU member states for the transposition of Directive 2001/55/EC and their influence on the real picture of refugee-immigration flows from Ukraine show dependencies between policies and migration dynamics. The observed deficits and irregularities in the transposition of the European Directive on temporary protection have the potential to differentiate the refugee masses, according to the mechanisms of their management (types of status), but at the same time lead to their concentration in certain countries, under the complex action of the pull factors.

All this, and the specifics of the refugee contingent, the lack of clarity about the end of hostilities and the absence of a European mechanism for long-term control of a mass influx of refugees, turn the Ukrainian refugee crisis into an open problem. It will inevitably divide the EU into nation states that must refer to their national legislations to resolve it. And this would be a decisive step towards the disintegration of the Union and perhaps the most effective hybrid-type weapon in the war against Europe.

#### REFERENCES

- [1] How many Ukrainian refugees are there and where have they gone? [How many Ukrainian refugees are there and where have they gone? - BBC News](#) [Accessed on 22.02.24]
- [2] Annual Report on Migration and Asylum 2022, Statistical Annex, Co-produced by Eurostat and the European Migration Network, June 2023. [EMN Annual Report on Migration and Asylum 2022 - Statistical Annex \(europa.eu\)](#) [Accessed on 22.02.24]
- [3] Infographic - Refugees from Ukraine in the EU. [Refugees from Ukraine in the EU - Consilium \(europa.eu\)](#) [Accessed on 22.02.24]
- [4] REGULATION (EU) 2017/371 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 1 March 2017 amending Council Regulation (EC) No 539/2001 listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement (revision of the suspension mechanism). [Regulation \(EU\) 2017/371 of the European Parliament and of the Council of 1 March 2017 amending Council Regulation \(EC\) No 539/2001 listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement \(revision of the suspension mechanism\) \(europa.eu\)](#) [Accessed on 22.02.24]
- [5] European Commission welcomes the Council adoption of visa liberalisation for the citizens of Ukraine, Statement, 17 May 2017, Brussels. [European Commission welcomes the Council adoption of visa liberalisation for the citizens of Ukraine \(europa.eu\)](#) [Accessed on 22.02.24]
- [6] COUNCIL DIRECTIVE 2001/55/EC of 20 July 2001 on minimum standards for giving temporary protection in the event of a mass influx of displaced persons and on measures promoting a balance of efforts between Member States in receiving such persons and bearing the consequences thereof. [eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001L0055](#) [Accessed on 22.02.24]
- [7] Convention from 1951 and Protocol from 1967 relating to the status of refugees, Geneva, UNHCR. [Convention and Protocol Relating to the Status of Refugees | UNHCR](#) [Accessed on 22.02.24]
- [8] Ukrainian citizens in the EU, Eurostat, *Data extracted in November 2022*. [Ukrainian citizens in the EU - Statistics Explained \(europa.eu\)](#) [Accessed on 23.02.24]

- [9] Ukrainians granted temporary protection in March 2022, Infographics, Eurostat, [78050567-93f5-d4cb-f904-4e9e9232103d\(2480x2480\) \(europa.eu\)](https://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&language=en&code=78050567-93f5-d4cb-f904-4e9e9232103d(2480x2480)(europa.eu)) [Accessed on 23.02.24]
- [10] Refugees in Ukraine, Infographics, European Council, [Refugees from Ukraine in the EU - Consilium \(europa.eu\)](https://ec.europa.eu/eu-external/en/refugees-from-ukraine-in-the-eu-consilium) [Accessed on 23.02.24]
- [11] Ukraine refugee situation, Operational Data Portal, [Situation Ukraine Refugee Situation \(unhcr.org\)](https://odp.unhcr.org/situation-ukraine-refugee-situation) [Accessed on 23.02.24]
- [12] Number of Ukrainian refugees with temporary protection status in EU grows by 36,600 in Nov – Eurostat, 15 Jan 2024, [Number of Ukrainian refugees with temporary protection status in EU grows by 36,600 in Nov - Eurostat \(interfax.com\)](https://www.interfax.com/en/news/number-of-ukrainian-refugees-with-temporary-protection-status-in-eu-grows-by-36-600-in-nov-eurostat) [Accessed on 23.02.24]
- [13] COUNCIL IMPLEMENTING DECISION (EU) 2022/382 of 4 March 2022 establishing the existence of a mass influx of displaced persons from Ukraine within the meaning of Article 5 of Directive 2001/55/EC, and having the effect of introducing temporary protection, [Publications Office \(europa.eu\)](https://eur-lex.europa.eu/eli/dec/2022/382/oj) [Accessed on 23.02.24]
- [14] COMMUNICATION FROM THE COMMISSION on Operational guidelines for the implementation of Council implementing Decision 2022/382 establishing the existence of a mass influx of displaced persons from Ukraine within the meaning of Article 5 of Directive 2001/55/EC, and having the effect of introducing temporary protection (2022/C 126 I/01), [Publications Office \(europa.eu\)](https://eur-lex.europa.eu/eli/dec/2022/126/i/01/oj) [Accessed on 23.02.24]
- [15] Worldwide/Ukraine: Temporary Protection Status - Country-Specific Updates, February 23, 2024, [Worldwide/Ukraine: Temporary Protection Status - Country-Specific Updates | Fragomen, Del Rey, Bernsen & Loewy LLP](https://www.fragomen.com/en/insights/worldwide-ukraine-temporary-protection-status-country-specific-updates) [Accessed on 23.02.24]
- [16] The potential contribution of Ukrainian refugees to the labour force in European host countries, 27 July 2022, [The potential contribution of Ukrainian refugees to the labour force in European host countries \(oecd.org\)](https://www.oecd.org/en/publications/2022/07/the-potential-contribution-of-ukrainian-refugees-to-the-labour-force-in-european-host-countries) [Accessed on 23.02.24]
- [17] ETIAS for Ukrainians, [ETIAS Europe Visa Waiver for Ukrainians - ETIASVisa.com](https://etiasvisa.com/en/etias-europe-visa-waiver-for-ukrainians) [Accessed on 24.02.24]
- [18] National legislation implementing the EU Temporary Protection Directive in selected EU Member States (October 2022 update), 31 October 2022, [National legislation implementing the EU Temporary Protection Directive in selected EU Member States \(October 2022 update\) | European Union Agency for Fundamental Rights \(europa.eu\)](https://www.efundamentalrights.europa.eu/en/national-legislation-implementing-the-eu-temporary-protection-directive-in-selected-eu-member-states-october-2022-update) [Accessed on 24.02.24]

# Analysis of the formation of cavitation cavity during the movement of a modified bullet of 7.62x39 ammunition in a water environment

**Blagovest Bankov**

Department of „Armament and Technology for Design“  
National Military University “Vasil Levski”  
Shumen, Bulgaria  
blagovest.bankov@gmail.com

**Abstract.** The report examines the behavior of a 7.62x39 bullet in a water environment and the changes in the created cavitation cavity when the geometric and mass characteristics are altered. The studies are conducted through virtual prototypes and CFD (Computational Fluid Dynamics) analyses in a SolidWorks environment, with the density of the water around the projectile and the angle of the formed cavitation cavities being the control parameters. The results indicate that the placement of the radial slit channel in the middle of the ogive part yields the best results for the angle of the cavitation cavity, which helps reduce the friction forces on the projectile, thereby increasing its linear progression in a water environment.

**Keywords:** Cavitation, CFD Analysis, 7.62x39 projectile, SolidWorks

## I. INTRODUCTION

In today's dynamic development of the geopolitical situation and the emergence of various disturbances around the world, there is a need for rapid development of new weapon systems and ammunition that can be used in complex situations, such as military operations where there may be a need to strike targets at different distances, including those under the water surface.

One of the challenges facing ammunition manufacturers is the development of an economically viable projectile with enhanced linear-progressive motion in a water environment, to meet the needs of users.

It is known that when a solid body enters water, its dynamics are disrupted by the impact of external forces and moments in the water environment, which reduces its translational and rotational motion [1], [2], [3].

Thanks to the development of computer technologies and mathematical models over the last decades, manufacturers have the opportunity to create virtual

prototypes of future or existing products [4], [5] [6], which can be tested in a virtual environment. This also provides the possibility of rapid physical prototyping [7], [8], [9] of a series of projectiles with altered geometric and mass characteristics, to study their behavior in a water environment.

With the help of a developed approach for virtually investigating the change in the angle of the created cavitation cavity during the motion of modified 7.62x54 ammunition in the studies [10] and [11], it is possible to track how the geometric and mass changes of a 7.62x39 projectile moving in water could affect the created cavitation bubble.

Cavitation is a phenomenon that generates cavities that grow and break up during the process of fluid flow when the local pressure is lower than the saturated vapor pressure [12].

Fig. 1 presents a diagram of the cavitation cavities formed when a projectile penetrates a water medium.

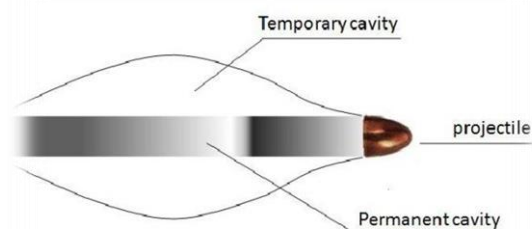


Fig. 1. Cavitation cavities [13].

The approach for studying the cavitation cavity, as used in this report, involves constructing a virtual model of the

Print ISSN 1691-5402  
Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8191>

© 2024 Blagovest Bankov. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).



bullet being researched and N number of variants with modified geometry, which consists of a slotted channel with a specific shape and dimensions in the ogive part of the projectile. The models are studied through CFD analysis, under the same conditions, and the formed angle between the bullet's axial line and a line starting from the ogive part of the bullet and ending at its base is compared. The slope is determined by an isoline showing the average water density zone (500 kg/m<sup>3</sup>) (Fig. 2), where it is considered that a cavitation cavity appears [14] [15] [16] [17].

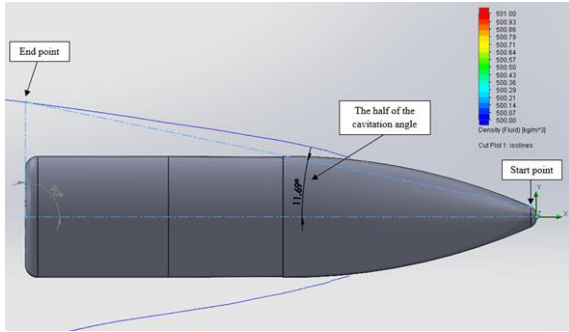


Fig. 2. Scheme of the study.

## II. MATERIALS AND METHODS

### A. Geometric modeling

The geometry of the projectile (Fig. 3) is designed based on a drawing with GRAU (system used by the Russian Armed Forces) index 57-N-231U, adopted in 1962 [18].

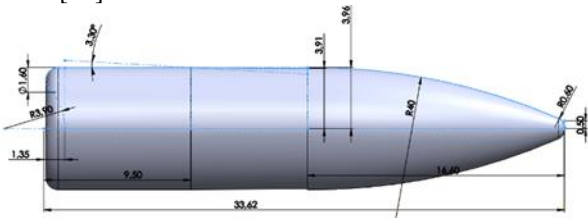


Fig. 3. The geometry of the projectile.

The shape and dimensions of the radially slotted channel of the bullets with altered geometric and mass characteristics are shown in Fig. 4, which are borrowed from the study [19], and the variations in its placement on the ogive part are shown in table 1.

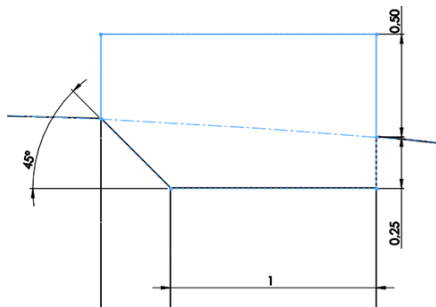


Fig. 4. The shape and dimensions of the radially slotted channel.

TABLE 1 VARIATIONS

Variation	1	2	3	4	5	6	7	8	9	10	11	12
Distance from top (mm)	0	3	4	5	6	7	8	9	10	11	12	13

Fig. 5 shows two variations of the projectile - (a) without a channel and (b) with a slotted channel.

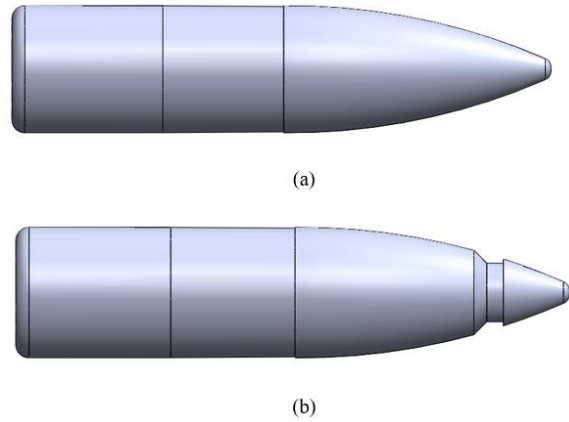


Fig. 5. Virtual models.

### B. Mesh model

The studied area is shown in Fig. 6, where the approach of constructing a 2D analysis is adopted due to the presence of rotational symmetry in the examined body. The number of finite elements in the studied area is 2024.

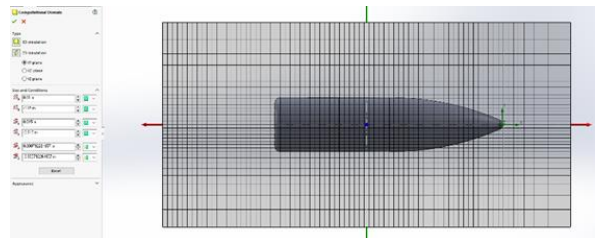


Fig. 6. The studied area.

### C. Input data

The following input data have been introduced for conducting the analysis:

- *Velocity* – the projectile's speed is assumed to be 715 m/s, corresponding to the initial velocity measured at 30 cm from the muzzle of the AKM-47 rifle [20];
- *Angular velocity* – the rotation speed is calculated using equation (1), which considers the rifling pitch in the barrel [21].

$$\omega_d = \pi \frac{V_d}{30S}, [s^{-1}], \quad (1)$$

where:

$V_d$  – translational velocity of the bullet [m/s];

$S$  – the rifling pitch in the barrel [m].

- *Dissolved gas mass fraction* – calculated with an equation (2) [19].

$$\sigma = 2 \frac{(P-P_0)}{\rho V^2} \quad (2)$$

where:

$P$  – atmospheric pressure at a temperature of 20°C [Pa];

$P_0$  – the pressure of the water vapor in the cavity (the approximate pressure is 0.02 atm [19]) [Pa];

$\rho$  – the density of water at a temperature of 20°C [kg/m<sup>3</sup>];

$V$  – the velocity of the projectile [m/s].

- *Turbulence Parameters* – turbulence intensity and length scale were calculated based on the length and speed of the projectile, and the kinematic viscosity of water, using the k-Epsilon model.

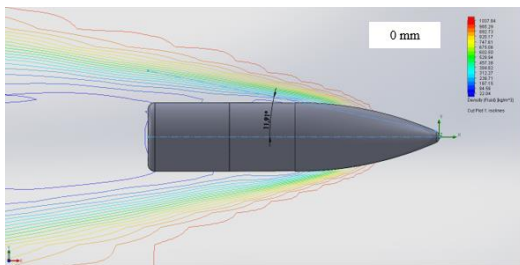
The input data introduced are shown in table 2.

TABLE 2 INPUT DATA

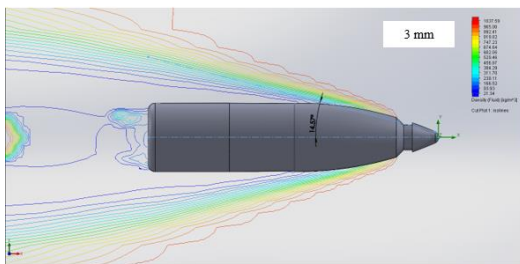
Parameter	Value	Dimension
Velocity	715	m/s
Angular velocity	32,67	rad/s
Dissolved gas mass fraction	0,000423099227	-
Temperature	293,2	K
Pressure	101325	Pa
Turbulence intensity	0,02552	%
Turbulence length	0,000234	m

### III. RESULTS AND DISCUSSION

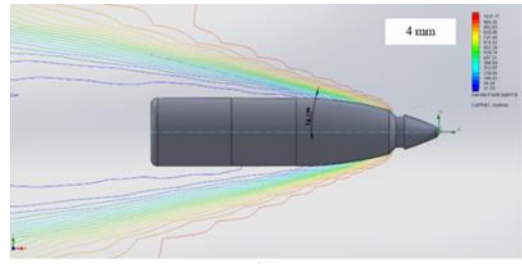
In Fig. 7 and Fig. 8, the results of the studies are presented graphically, showing the angles of the formed cavitation cavities, and in Fig. 9 all the obtained angles are compared, demonstrating that the best results are achieved when the slotted channel is positioned 7 mm from the tip of the bullet.



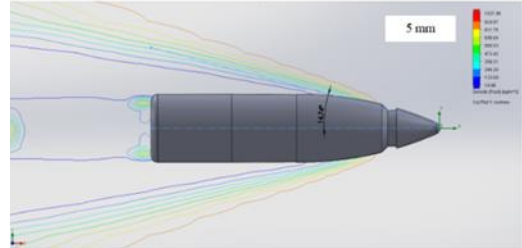
(a)



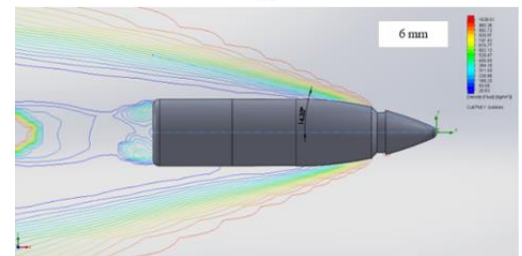
(b)



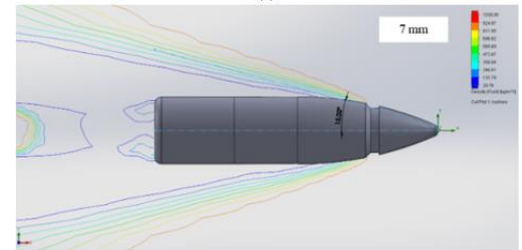
(c)



(d)

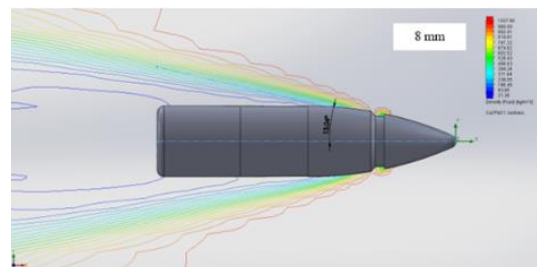


(e)

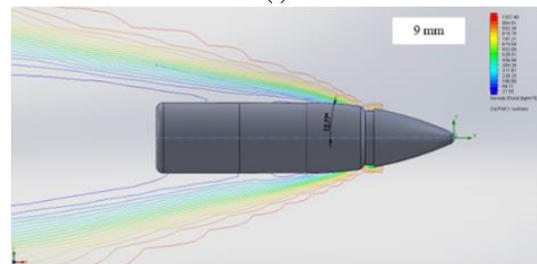


(f)

Fig. 7. Result - first part.



(a)



(b)

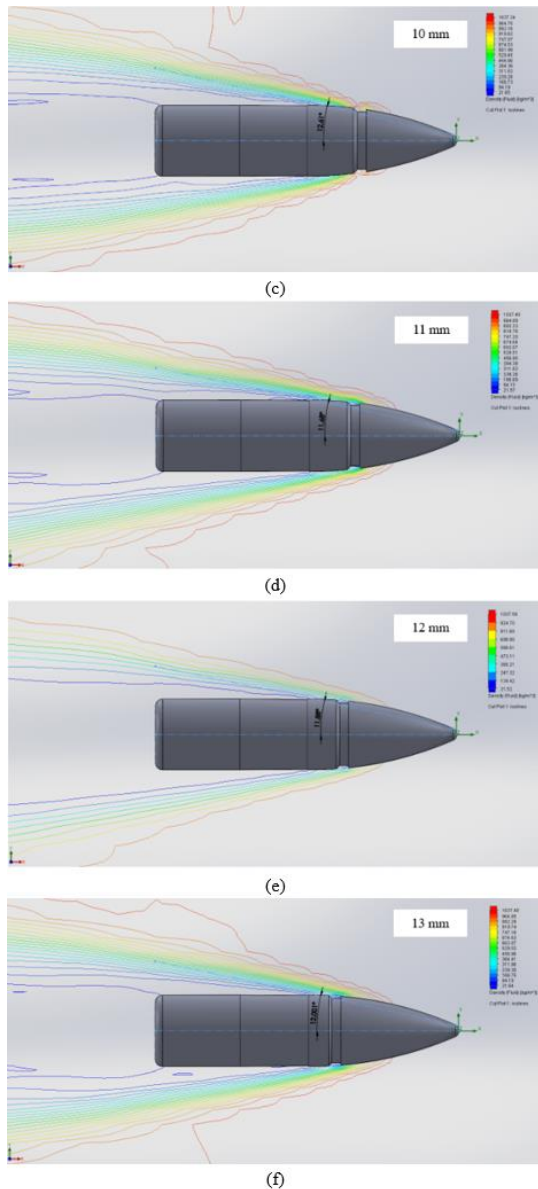


Fig. 8. Result - second part.

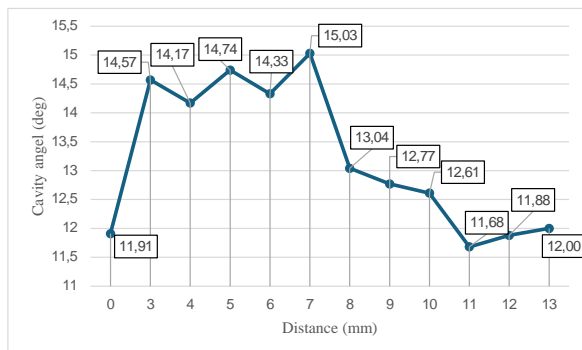


Fig. 9. The angle of the cavitation cavity vs. notch the distance from the tip of the bullet.

#### IV. CONCLUSION

- The study found that the placement of the slit channel near the middle of the live part yields the best results for the angle of the cavitation cavity, which would help reduce the forces negatively affecting the dynamics

of the projectile, thereby extending its translational movement in a water medium.

- The results from positioning the cut more than 10 mm from the tip of the bullet are approximately the same as those of the projectile without a radial cut.
- Thanks to virtual prototyping, it is possible to analyze various projectile variations with changed geometry and mass characteristics, which in turn accelerates the process of developing new ammunition.

#### ACKNOWLEDGMENTS

The report is being carried out under the National Scientific Program "Security and Defense," adopted by Council of Ministers Decree № 731 of October 21, 2021, and in accordance with Agreement № D01-74/19.05.2022.



#### REFERENCES

- V.-T. Nguyen, T.-H. Phan, and W.-G. Park, 'Modeling and numerical simulation of ricochet and penetration of water entry bodies using an efficient free surface model', *International Journal of Mechanical Sciences*, vol. 182, p. 105726, Sep. 2020, doi: 10.1016/j.ijmecsci.2020.105726.
- S. Liu, C. Xu, Y. Wen, S. Wang, J. Zhou, and X. Zhou, 'Cavity dynamics in 10 wt% gelatin penetration of rifle bullet', *International Journal of Impact Engineering*, vol. 122, pp. 296–304, Dec. 2018, doi: 10.1016/j.ijimpeng.2018.09.006.
- G.-X. Yan, G. Pan, Y. Shi, L.-M. Chao, and D. Zhang, 'Experimental and numerical investigation of water impact on air-launched AUVs', *Ocean Engineering*, vol. 167, pp. 156–168, Nov. 2018, doi: 10.1016/j.oceaneng.2018.08.044.
- Y. Sofronov, M. Zagorski, G. Todorov, and T. Gavrilov, 'Approach for reverse engineering of complex geometry components', presented at the *BulTrans*, Sozopol, Bulgaria, 2019.
- S. Antonov, 'Modern technologies in computer design and application of systems for stress-strain calculations of weapon system elements', presented at the *International Conference knowledge-based organization*, 2020.
- K. Lukaszewicz, 'Use of CAD Software in the Process of Virtual Prototyping of Machinery', *Procedia Engineering*, vol. 182, pp. 425–433, 2017, doi: 10.1016/j.proeng.2017.03.127.
- Y.-M. Huang and H.-Y. Lan, 'CAD/CAE/CAM integration for increasing the accuracy of mask rapid prototyping system', *Computers in Industry*, vol. 56, no. 5, pp. 442–456, Jun. 2005, doi: 10.1016/j.compind.2005.01.002.
- A. Fischer, 'Multi-level models for reverse engineering and rapid prototyping in remote CAD systems', *Computer-Aided Design*, vol. 32, no. 1, pp. 27–38, Jan. 2000, doi: 10.1016/S0010-4485(99)00081-0.
- K. Subburaj, C. Nair, S. Rajesh, S. M. Meshram, and B. Ravi, 'Rapid development of auricular prosthesis using CAD and rapid prototyping technologies', *International Journal of Oral and Maxillofacial Surgery*, vol. 36, no. 10, pp. 938–943, Oct. 2007, doi: 10.1016/j.ijom.2007.07.013.
- V. Ganev, R. Lazarov, and B. Bankov, 'Approach for determining the ballistic characteristics of the ammunition', presented at the *International Scientific Conference —Defense Technologies*, Shumen, 2023, pp. 285–289.
- V. Ganev and B. Bankov, 'Investigation of the motion of a 7,62x54 caliber projectile in an aquatic environment', presented at the *Актуални проблеми на сигурността*, Велико Търново: Издателски комплекс на НВУ „Васил Левски“, 2023, pp. 1511–1516.
- H. Fang and M. Duan, 'Special Problems of Deep-Sea Oil and Gas Engineering', in *Offshore Operation Facilities*, Elsevier, 2014, pp. 537–686. doi: 10.1016/B978-0-12-396977-4.00004-4.
- P. Lichte, R. Oberbeck, M. Binnebösel, R. Wildenauer, H.-C. Pape, and P. Kobbe, 'A civilian perspective on ballistic trauma and gunshot

- injuries', *Scand J Trauma Resusc Emerg Med*, vol. 18, no. 1, p. 35, 2010, doi: 10.1186/1757-7241-18-35.
- [14] F. Magaletti, M. Gallo, and C. M. Casciola, 'Water cavitation from ambient to high temperatures', *Sci Rep*, vol. 11, no. 1, p. 20801, Oct. 2021, doi: 10.1038/s41598-021-99863-z.
- [15] F. Caupin and E. Herbert, 'Cavitation in water: a review', *Comptes Rendus Physique*, vol. 7, no. 9–10, pp. 1000–1017, Nov. 2006, doi: 10.1016/j.crhy.2006.10.015.
- [16] C. E. Brennen, *Cavitation and Bubble Dynamics*. Cambridge: Cambridge University Press, 2013. doi: 10.1017/CBO9781107338760.
- [17] D. H. Trevena, 'Cavitation and the generation of tension in liquids', *J. Phys. D: Appl. Phys.*, vol. 17, no. 11, pp. 2139–2164, Nov. 1984, doi: 10.1088/0022-3727/17/11/003.
- [18] EOD, '7.62x39 green black tip factory 711', International Ammunition Association, Inc. Accessed: Jan. 05, 2024. [Online]. Available: <https://forum.cartridgecollectors.org/t/7-62x39-green-black-tip-factory-711/38421>
- [19] Р. Лазаров, 'Изследване на влиянието на формата на куршума върху рикошетното му действие', НВУ 'Васил Левски', Велико Търново, 2022.
- [20] Министерство на народната отбрана, *Наставление по стрелково дело. Материална част на стрелково оръжие*. София: Военно издателство, 1987.
- [21] Я. Димитрова, 'Изследване на влиянието на трибологичните характеристики на шумозаглушител върху групиралността при стрелба със стрелково оръжие.', НВУ "Васил Левски", Велико Търново, 2021.

# Analysis of the influence of the ogive radius of a 7.62x39 ammunition bullet on the cavitation cavity

**Blagovest Bankov**

Department of „Armament and Technology for Design“  
National Military University “Vasil Levski”  
Shumen, Bulgaria  
blagovest.bankov@gmail.com

**Abstract.** The aim of the current study is to examine the impact of the ogive radius of a 7.62x39 ammunition projectile on the positioning of a radially-slotted channel that helps increase the angle of the cavitation cavity. The studies were conducted using CFD (Computational Fluid Dynamics) analyses in a SolidWorks environment, simulating the projectile's movement in a water environment. The research findings indicate that lower values of the ogive radius result in higher values of the cavitation cavity angle, which in turn suggests that lower values are more favorable for creating bullets with slotted channels, which enhances linear-progressive movement in a water environment and thus increases the chance of hitting targets below sea level.

**Keywords:** Cavitation, CFD Analysis, SolidWorks, 7.62x39 projectile

## I. INTRODUCTION

Through the development of computing power, various mathematical models, and software products for virtual prototyping and research, there is an opportunity for faster analysis of problems of any nature. The possibility of designing future and existing products using Reverse Engineering techniques and the assistance of various CAD (Computer Aided Design) software products in a virtual environment opens potential directions for the development of products from a wide range of fields [1] [2] [3] [4] [5] [6] [7] [8] [9] [10].

Apart from the broad and well-known industry, design and analysis software is also used for creating weapon systems, as well as for developing new types of ammunition. One of the issues considered in the military industry is increasing the range of bullets in a water medium.

When a solid body enters a water medium, its dynamics are disrupted due to various forces, significantly

reducing its movement [11] [12] [13] [14]. It is also known that when a solid body moves at a sufficiently high speed under water, pressure around the body itself is created, which is lower than the pressure of the saturated steam in the surrounding water, thus forming a cavity that can encompass a large part of the body. When super cavitation occurs, only a small part of the body is in contact with the steam and the formed cavity [15] [16] [17] [18] [19] [20].

The use of specialized software products for virtual analyses, collectively known as “Computer Aided Engineering” (CAE), and specifically those allowing fluid analyses (CFD, Computational Fluid Dynamics), enable manufacturers, researchers, and designers to study various processes [21] [22] [23] [24] [25], such as cavitation, thereby improving existing products or producing new prototypes [26] [27].

With the help of a developed method using CFD analysis for virtual study of the change in the angle of the created cavitation cavity during the movement of a modified projectile of ammunition 7.62x54, shown in the studies [28] and [29], it is possible to examine the influence of the ogive radius of a 7.62x39 bullet on the angle of the cavitation cavity, as well as on the positioning of a radially slotted channel, which aims to increase the values of the cavity angle.

The approach consists in designing n number of virtual models, which are subjected to identical input data and the resulting angle of the cavitation cavity is examined, which is measured by the angle formed between two lines - the axial line of the projectile and a line starting from the ogive part of the bullet and ending at its base, where the slope is determined by an isoline, showing the average water density zone (500 kg/m<sup>3</sup>) (Fig. 1), at which it is considered that a cavitation cavity appears [16] [17] [18] [19].

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8192>

© 2024 Blagovest Bankov. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

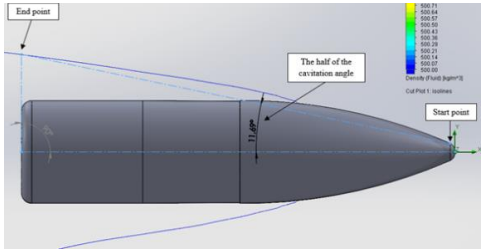


Fig. 1. Scheme of the study.

## II. MATERIALS AND METHODS

### A. Geometric modeling

Virtual prototypes of a 7.62x39 mm ammunition projectile with various ogive radii, ranging from R40 to R80, have been designed (Fig. 2).

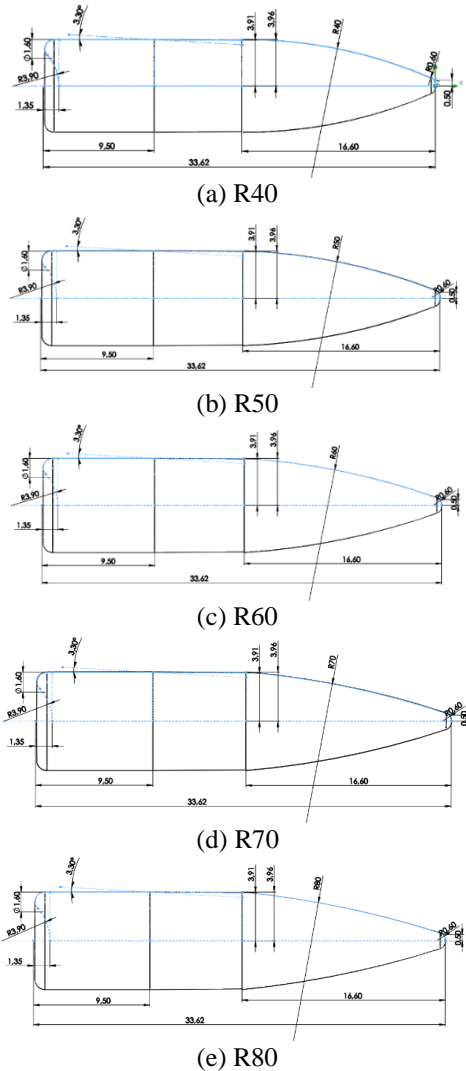


Fig. 2. Geometric models.

The shape and dimensions of the radially slotted channel are shown in Fig. 3, as they are adopted from the work [30].

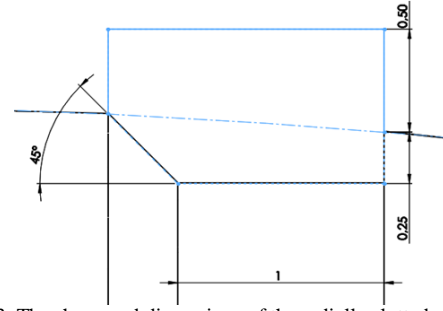


Fig. 3. The shape and dimensions of the radially slotted channel.

### B. Mesh model

A two-dimensional finite element mesh model has been constructed due to the rotational symmetry of the body under study. The model consists of 2024 finite elements (Fig. 4). An approach with an adaptive mesh has been chosen, with a Ratio Factor of 3.5 for densifying the mesh around the ogive and the radially slotted channel.

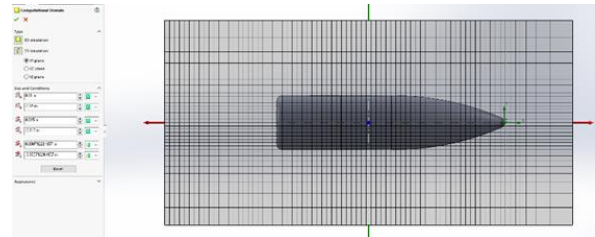


Fig. 4. The studied area.

### C. Input data

The following input data have been introduced for conducting the analysis:

- *Velocity* – the projectile's speed is assumed to be 715 m/s, corresponding to the initial velocity measured at 30 cm from the muzzle of the AKM-47 rifle [31];
- *Angular velocity* – the rotation speed is calculated using equation (1), which considers the rifling pitch in the barrel [32].

$$\omega_d = \pi \frac{V_d}{30S}, [s^{-1}], \quad (1)$$

where:

$V_d$  – translational velocity of the bullet [m/s];

$S$  – the rifling pitch in the barrel [m].

- *Dissolved gas mass fraction* – calculated with an equation (2).

$$\sigma = 2 \frac{(P-P_0)}{\rho V^2}, \quad (2)$$

where:

$P$  – atmospheric pressure at a temperature of 20°C [Pa];

$P_0$  – the pressure of the water vapor in the cavity (the approximate pressure is 0.02 atm [30]) [Pa];

$\rho$  – the density of water at a temperature of 20°C [kg/m<sup>3</sup>];

$V$  – the velocity of the projectile [m/s].

- *Turbulence intensity* - this parameter is calculated based on the k-Epsilon model using equation (3).

$$TI = \sqrt{\frac{2k}{3}} \frac{1}{U}, \quad (3)$$

where:

$U$  - the average velocity of the fluid [m/s];

$k$  - the turbulent kinetic energy per unit volume, which within the k-Epsilon model is determined relative to the length of the body (in this case, the bullet), the velocity of the fluid, and the kinematic viscosity of the fluid.

• *Length scale* - The value is calculated based on equation (4).

$$LC = C_{\mu} \frac{k^{\frac{2}{3}}}{\epsilon}, \quad (4)$$

where:

$C_{\mu}$  - is the constant in the k-Epsilon model and has a value of 0.09 [33];

$k$  - the turbulent kinetic energy per unit volume;

$\epsilon$  - the rate of dissipation, whose approximate value can be found using formula (5).

$$\epsilon \approx \frac{V^3}{L} \quad (5)$$

where:

$V$  - fluid velocity [m/s];

$L$  - length of the body [m]

The summarized input data can be seen in table 1.

TABLE 1 INPUT DATA

Parameter	Value	Dimension
Velocity	715	m/s
Angular velocity	32,67	rad/s
Dissolved gas mass fraction	0,000423099227	-
Temperature	293,2	K
Pressure	101325	Pa
Turbulence intensity	0,02552	%
Turbulence length	0,000234	m

### III. RESULTS AND DISCUSSION

In Fig. 5, a diagram is shown that compares the results from all the analyses of the angles of the cavitation cavity, and in table 2, their numerical values are provided.

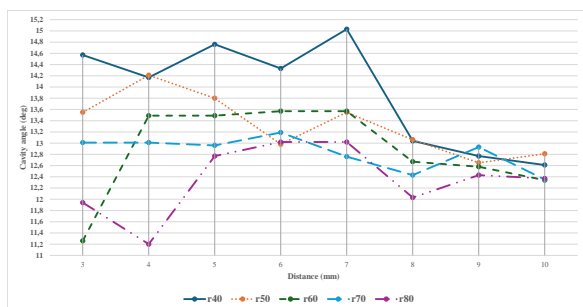


Fig. 5. The angle of the cavitation cavity vs. notch the distance from the tips of the bullets.

In the conducted analyses, a trend of decreasing the angle of the cavitation cavity was observed with the increase in the ogive radius. Upon closer examination of the section with the radially slotted channel at 7mm from

the tip of the projectile, in the models with radii r40 and r80, it was found that the lower radius creates higher fluid vortices in the channel (Fig. 6) in zone 1 (Fig. 7).

TABLE 2 THE CAVITY CAVITIES ANGLES

R mm	R40	R50	R60	R70	R80
3	14,57	13,55	11,26	13,01	11,94
4	14,17	14,21	13,49	13,01	11,20
5	14,76	13,8	13,49	12,96	12,77
6	14,33	12,98	13,57	13,19	13,02
7	15,03	13,55	13,57	12,76	13,02
8	13,04	13,06	12,67	12,43	12,03
9	12,77	12,65	12,58	12,93	12,43
10	12,61	12,81	12,34	12,35	12,37

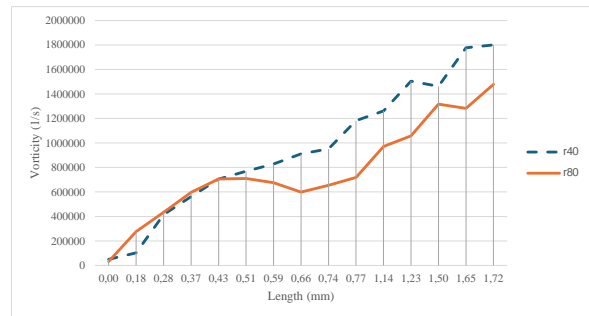


Fig. 6. Vorticity.

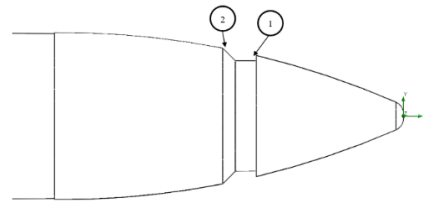


Fig. 7. Considered areas.

When examining the pressure in the same section, a lower pressure is observed in the model with a 40 mm radius (Fig. 8), where in zone 2 it increases by nearly 20 MPa, which could be attributed to the vortices that have formed.

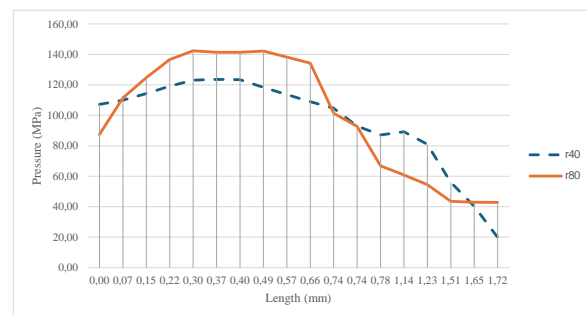


Fig. 8. Pressure results.

The fluid density in zones 1 and 2 has also been examined, with lower values observed in the model with an ogive of r40 (Fig. 9).

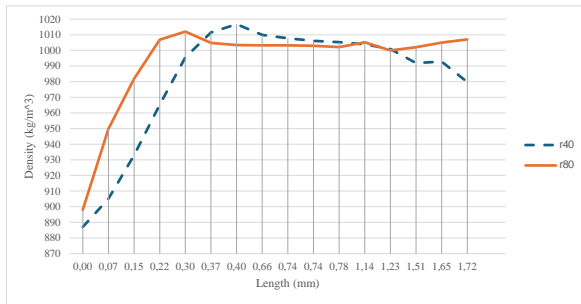


Fig. 9. Density results.

#### IV. CONCLUSION

- Radial channels that are 8 mm and above are less efficient in creating a cavitation cavity.
- The most suitable positioning of radial channels along the ogive part is in the area from 5 to 7 mm from the tip of the bullet.
- Approximately 10% better values are observed with the ogive of r40 when the radial channel is positioned between 5 and 7 mm compared to the same positioning but with an ogive radius of r60 to r80.
- Additional research on a projectile with an ogive radius of 40 mm and a projectile with a radius of 80 mm confirms the hypothesis that lower values of the ogive radius influence the nature of the cavitation cavity, and the creation of radial slotted channels in the middle zone of the ogive facilitates its expansion.

#### ACKNOWLEDGMENTS

The report is being carried out under the National Scientific Program "Security and Defense," adopted by Council of Ministers Decree № 731 of October 21, 2021, and in accordance with Agreement № D01-74/19.05.2022.

#### REFERENCES

[1] S. Antonov, 'Modern technologies in computer design and application of systems for stress-strain calculations of weapon system elements', presented at the International Conference knowledge-based organization, 2020.

[2] Y. A. Hosni, 'Contribution of CAD-CAM and reverse engineering technology to the biomedical field', in *Current Advances in Mechanical Design and Production VII*, Elsevier, 2000, pp. 491–499. doi: 10.1016/B978-008043711-8/50050-7.

[3] I. Kovács, T. Várady, and P. Salvi, 'Applying geometric constraints for perfecting CAD models in reverse engineering', *Graphical Models*, vol. 82, pp. 44–57, Nov. 2015, doi: 10.1016/j.gmod.2015.06.002.

[4] K. Łukaszewicz, 'Use of CAD Software in the Process of Virtual Prototyping of Machinery', *Procedia Engineering*, vol. 182, pp. 425–433, 2017, doi: 10.1016/j.proeng.2017.03.127.

[5] A. Raffo, O. J. D. Barrowclough, and G. Muntingh, 'Reverse engineering of CAD models via clustering and approximate implicitization', *Computer Aided Geometric Design*, vol. 80, p. 101876, Jun. 2020, doi: 10.1016/j.cagd.2020.101876.

[6] D. W. Rosen, N. Jeong, and Y. Wang, 'A method for reverse engineering of material microstructure for heterogeneous CAD', *Computer-Aided Design*, vol. 45, no. 7, pp. 1068–1078, Jul. 2013, doi: 10.1016/j.cad.2013.01.004.

[7] M. Rozesara, S. Ghazinoori, M. Manteghi, and S. H. Tabatabaiean, 'A reverse engineering-based model for innovation process in complex product systems: Multiple case studies in the aviation industry', *Journal of Engineering and Technology Management*, vol. 69, p. 101765, Jul. 2023, doi: 10.1016/j.jengtecman.2023.101765.

[8] Y. Sofronov, M. Zagorski, G. Todorov, and T. Gavrilov, 'Approach for reverse engineering of complex geometry components', presented at the *BulTrans*, Sozopol, Bulgaria, 2019.

[9] M. Zagorski, G. Todorov, N. Nikolov, Y. Sofronov, and M. Kandevara, 'Investigation on wear of biopolymer parts produced by 3D printing in lubricated sliding conditions', *ILT*, vol. 74, no. 3, pp. 360–366, Mar. 2022, doi: 10.1108/ILT-06-2021-0214.

[10] B. S. Rupal, K. G. Mostafa, Y. Wang, and A. J. Qureshi, 'A Reverse CAD Approach for Estimating Geometric and Mechanical Behavior

of FDM Printed Parts', *Procedia Manufacturing*, vol. 34, pp. 535–544, 2019, doi: 10.1016/j.promfg.2019.06.217.

[11] J. A. Batlle and A. Barjau Condomines, *Rigid Body Dynamics*, 1st ed. Cambridge University Press, 2022. doi: 10.1017/9781108896191.

[12] V.-T. Nguyen, T.-H. Phan, and W.-G. Park, 'Modeling and numerical simulation of ricochet and penetration of water entry bodies using an efficient free surface model', *International Journal of Mechanical Sciences*, vol. 182, p. 105726, Sep. 2020, doi: 10.1016/j.ijmecsci.2020.105726.

[13] S. Liu, C. Xu, Y. Wen, S. Wang, J. Zhou, and X. Zhou, 'Cavity dynamics in 10 wt% gelatin penetration of rifle bullet', *International Journal of Impact Engineering*, vol. 122, pp. 296–304, Dec. 2018, doi: 10.1016/j.ijimpeng.2018.09.006.

[14] G.-X. Yan, G. Pan, Y. Shi, L.-M. Chao, and D. Zhang, 'Experimental and numerical investigation of water impact on air-launched AUVs', *Ocean Engineering*, vol. 167, pp. 156–168, Nov. 2018, doi: 10.1016/j.oceaneng.2018.08.044.

[15] V. R. Feldgun, D. Z. Yankelevsky, and Y. S. Karinski, 'Cavitation phenomenon in penetration of rigid projectiles into elastic-plastic targets', *International Journal of Impact Engineering*, vol. 151, p. 103837, May 2021, doi: 10.1016/j.ijimpeng.2021.103837.

[16] F. Magaletti, M. Gallo, and C. M. Casciola, 'Water cavitation from ambient to high temperatures', *Sci Rep*, vol. 11, no. 1, p. 20801, Oct. 2021, doi: 10.1038/s41598-021-99863-z.

[17] F. Caupin and E. Herbert, 'Cavitation in water: a review', *Comptes Rendus Physique*, vol. 7, no. 9–10, pp. 1000–1017, Nov. 2006, doi: 10.1016/j.crh.2006.10.015.

[18] C. E. Brennen, *Cavitation and Bubble Dynamics*. Cambridge: Cambridge University Press, 2013. doi: 10.1017/CBO9781107338760.

[19] D. H. Trevena, 'Cavitation and the generation of tension in liquids', *J. Phys. D: Appl. Phys.*, vol. 17, no. 11, pp. 2139–2164, Nov. 1984, doi: 10.1088/0022-3727/17/11/003.

[20] J. S. Carlton, 'Cavitation', in *Marine Propellers and Propulsion*, Elsevier, 2012, pp. 209–250. doi: 10.1016/B978-0-08-097123-0.00009-5.

[21] J. Hua et al., 'Recent development of a CFD-wind tunnel correlation study based on CAE-AVM investigation', *Chinese Journal of Aeronautics*, vol. 31, no. 3, pp. 419–428, Mar. 2018, doi: 10.1016/j.cja.2018.01.017.

[22] R. Molinaro, J.-S. Singh, S. Catsoulis, C. Narayanan, and D. Lakehal, 'Embedding data analytics and CFD into the digital twin concept', *Computers & Fluids*, vol. 214, p. 104759, Jan. 2021, doi: 10.1016/j.compfluid.2020.104759.

[23] E. Henriksen, P. Wood, and K. Hanna, 'Utilization of integrated CAD/CAE computational fluid dynamic tools in the golf driver design process', *Procedia Engineering*, vol. 34, pp. 68–73, 2012, doi: 10.1016/j.proeng.2012.04.013.

[24] S. Aram and P. Mucha, 'CFD validation and analysis of turning maneuvers of a surface combatant in regular waves', *Ocean Engineering*, vol. 293, p. 116653, Feb. 2024, doi: 10.1016/j.oceaneng.2023.116653.

[25] G. Todorov, K. Kamberov, and T. Ivanov, 'Parametric optimisation of resistance temperature detector design using validated virtual prototyping approach', *Case Studies in Thermal Engineering*, vol. 28, p. 101302, Dec. 2021, doi: 10.1016/j.csite.2021.101302.

[26] F. Orlandi, L. Montorsi, and M. Milani, 'Cavitation analysis through CFD in industrial pumps: A review', *International Journal of Thermofluids*, vol. 20, p. 100506, Nov. 2023, doi: 10.1016/j.ijft.2023.100506.

[27] S. Ahmed, A. Hassan, R. Zubair, S. Rashid, and A. Ullah, 'Design modification in an industrial multistage orifice to avoid cavitation using CFD simulation', *Journal of the Taiwan Institute of Chemical Engineers*, vol. 148, p. 104833, Jul. 2023, doi: 10.1016/j.jtice.2023.104833.

[28] V. Ganev, R. Lazarov, and B. Bankov, 'Approach for determining the ballistic characteristics of the ammunition', presented at the *International Scientific Conference —Defense Technologies*, Shumen, 2023, pp. 285–289.

[29] V. Ganev and B. Bankov, 'Investigation of the motion of a 7,62x54 caliber projectile in an aquatic environment', presented at the *Актуални проблеми на сигурността, Велико Търново: Издателски комплекс на НВУ „Васил Левски“*, 2023, pp. 1511–1516.

[30] P. Lazarov, 'Изследване на влиянието на формата на куршума върху рикошетното му действие', НВУ "Васил Левски", Велико Търново, 2022.

[31] Министерство на народната отбрана, *Наставление по стрелково дело. Материална част на стрелково оръжие*. София: Военно издателство, 1987.

[32] Я. Димитрова, 'Изследване на влиянието на трибологичните характеристики на шумозаглушител върху групиранията при стрелба със стрелково оръжие.', НВУ "Васил Левски", Велико Търново, 2021.

[33] CFD Wiki, 'Turbulence length scale', *CFD Online*. Accessed: Jan. 21, 2024. [Online]. Available: [https://www.cfd-online.com/Wiki/Turbulence\\_length\\_scale](https://www.cfd-online.com/Wiki/Turbulence_length_scale)



# *The importance of designing of information systems and data exchange possibilities to carry out multidisciplinary cooperation to prevent violence against children*

**Ilze Bērziņa**  
Faculty of Social Sciences  
Riga Stradiņš University  
Riga, Latvia  
ilze.berzina@rsu.lv

**Abstract.** We live in a modern society where institutions have their data systems and databases. They are used to organize the internal work of the institution with the aim to serve people and the community. Almost each of the state institutions are having its own unique way to gather and collect data and it does not always mean that it is possible to connect these data or use them by all involved partners during multidisciplinary and multisectoral cooperation. Do these data systems serve people or do people “serve” them? Are these data useful and accessible to carry out research and to make policy conclusions and have cost-benefit analysis? The author is analyzing available data from the perspective of different aims of research, including cost-benefit analysis, which is not a widely used method in Latvia, especially, in the field of criminal justice. The article is also modeling the situational analysis in the case where there is a need to carry out crime prevention activities and rehabilitation for the victim of violence and how the implementation of Barnahus model can support that. How do institutions exchange data? Can they have access to the data systems and do these technologies serve the community and children? The answer is simple – the keyword is still humanity and the human aspect is still the main to make sure that data systems and databases are serving people and not vice versa.

**Keywords:** *Barnahus, Cost benefit analysis, Crime prevention, Data protection and exchange of data, Information systems for people, Multidisciplinary cooperation.*

## I. INTRODUCTION

The Conference Article is devoted to the analysis and research in connection with the implementation of Barnahus model (delivered from the Icelandic for “children’s house”). Which, according to the definition given by Promise, Barnahus Network in the Council of Europe, is a child-friendly, multidisciplinary and interagency model for responding to child violence and witnesses of violence in Latvia and the importance of the design of the information systems and data exchange possibilities among institutions. Barnahus, initially brought to Europe in Iceland and Nordic countries, is well known all over EU and is now being implemented in Latvia. Recently passed changes in the Law on Protection of the Rights of the Child and regulations of the Cabinet of Ministers about the work of Barnahus in Latvia states the system and way how the program and service is implemented and cooperation is carried out between medical institutions, police and other law enforcement institutions, social service, and child care institutions.

Data about violence against children in Latvia are gathered by several institutions – NGOs, police and court system, social services and medical institutions. In order to make any conclusions, it is necessary to look for the available data in all publicly accessible databases and they are not giving the “full picture”, not even in one segment (Berzina, 2023<sup>7</sup>). However, many researchers and policy analytics are concluding that data are fragmented (Baltic institute of Social Sciences, 2023<sup>5</sup>) and not comparable for policy planning. (OECD, 2023<sup>3</sup>) The author is also modelling the situations from possible cases in Barnahus in order to see a real application of the databases for crime prevention and if it is in the best interest of the child. It is concluded that there are a lot of gaps and weaknesses in the real situation and the need for

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8242>

© 2024 Ilze Bērziņa. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

human aspect is still remaining as the most important to solve the cases. It is essential that design of the information systems should be done in a way that would make it easier to use them in multisectoral cooperation.

The aim of the article is also to analyze the available information and policy documents, including the OECD (OECD, Towards a Child-Friendly Justice system in Latvia: Support to the Implementation of Barnahus in Latvia”, 2023<sup>3</sup>), Report of the National Ombudsmen Tiesībsargs (Tiesībsargs, 2021<sup>2</sup>), available policy documents of the Council of Europe, European Commission and national policy documents to see what is the situation concerning the different ways and methods and evaluate the efficiency and cost-benefit analysis of the implementation of Barnahus model in Latvia. However, all of them show the necessity to improve existing practices, to gather data, and maintain data systems so that they can be used better for-policy planning and to serve the community.

## II. MATERIALS AND METHODS

The author is analyzing available data and research publications about violence against children from the perspective of different aims of research, including cost-benefit analysis, which is not a widely used method in Latvia, especially, in the field of criminal justice. The article is also modeling the situational analysis in the case where there is a need to carry out multidisciplinary cooperation and or rehabilitation for the victim of violence. By application of these methods we can see how Barnahus model can support crime prevention and how important is to exchange data or have access to them. During the modeling of case study of examples are provided to prove the necessity to improve existing practices as well to seek new methods and always have a personal and professional approach to each case.

## III. RESULTS AND DISCUSSION

### *A. WHY DATA AND DATA SYSTEMS ARE IMPORTANT FOR MULTIDISCIPLINARY COOPERATION?*

Nowadays information systems and databases play an important role in any field of our lives. It is even more important in the case of multidisciplinary and multisectoral cooperation and the reasons are very simple. Cooperation needs information, but the information is available mainly online and fast pace of everyday life is asking for a quick and effective exchange of data.

Even though various statistical systems are in place in Latvia, it has been mentioned by several local and international experts that stakeholders reported concerns related to the quality of data collection and the consistency of evaluations of programs on child-friendly justice. In the latest research carried out by OECD, it was concluded that data is collected in an unsystematic fashion through a range of uncoordinated separate mechanisms, such as police and school records, as well as those kept by social services and health workers. There appears to be no systematic way through which such records are collected and utilized to inform policy development. In the meantime, Data protection laws are protecting the ideal to connect all of these data automatically, because we are talking about the sensitive

data (Data protection Law of the Republic of Latvia, 2018<sup>1</sup>) Data are also secured and must be processed according to EU regulation (Regulation (EU) 2016/679, 2016<sup>4</sup>). In addition, there is room to strengthen data quality, sufficiency, and governance, particularly at the municipal level (OECD, Assessment, and recommendations for a child-friendly justice system in Latvia, 2023<sup>3</sup>).

Fragmentation of data and databases and also technical problems to connect and merge them are also mentioned in the most recent research carried out by the Ministry of Welfare (Baltic Institute of Social Sciences, 2023<sup>5</sup>). However, through the years the problem still remains unresolved and researchers and practitioners are the ones who try to make changes in the state policy.

From the point of view of specialists from the different professions in Barnahus there are several aspects:

- decision by the specialist to report the case of violence and enter the initial data in the system, for example, medical personnel (Berzina, 2023<sup>7</sup>);
- connection of different data in one system between specialists in the different institutions and also justification to access the data, if the systems are connected or not connected;
- technical solutions, information systems, and possibilities to seek and find information in one platform;
- human aspect is the most important – initiative to seek and ask for more information is in the best interests of the child and that is crucial.

### *B. CASE EXAMPLES*

During the semi structured interviews multiple situations or case studies were revealed. Here are three situations concerning the multisectoral and multidisciplinary cooperation.

The first case is very simple and quite typical – a child A with serious injuries is in the main hospital of Riga and all the data about the health and possible violence are recorded in the electronic system of the hospital, but medical databases are not connected between the regional hospital systems nor other systems. Specialist X (court expert) is making –expertise in the case and needs a full picture of the situation, including past situations with the child. From one point - data protection and security of sensitive data must be applied. According to the interviews with court experts, if the initiative is not taken in gathering of additional information, i.e. information about the previous episodes in regional hospitals or elsewhere, it might not be added to the main case and can delay the whole process. Specialist X needs to contact and write to the institutions, wait for long periods and add additional justifications to access the data and information. Result – effective investigation in the best interests of the child according to the article 3 of the UN Convention of the rights of the Child (UN Convention on the Rights of the Child, 2008<sup>6</sup>) is failing. If specialist doesn't practice due diligence, the case suffers even more. Of course, situations vary, but

each time human aspect and initiative to gather the information matters.

The second case (child B) is about early prevention. Social work and discussion about the united data system supporting cooperation between the several multidisciplinary players, schools, social workers, child care institutions, and other players matters a lot. It is about the national plans to further develop the national database system NPAIS (Information Support System for Juveniles) which was launched many years ago and still is not doing what it is supposed to and is not used for what it was created – to have multiple data from the different institutions. It should first signal about crime and be used for early crime prevention. In the case with the child B, information was needed to gather the initial information about the child, but specialists in Barnahus have no access to the system or to the SOPA system (Social Service Database System). Besides, there are several national systems for social services – Riga city has one system, but regions have other systems. It means, that to get to know about past situations, records from schools or social services about the family and household of the child, that could help in the early prevention of crime, all the information has to be collected manually and by the initiative of caseworker by approaching multiple specialists individually. Investigations prolong if families live in different places and it is a very common situation. It goes in total contradiction with the declared wishful thinking of the politicians about early crime prevention and policy strategies. We can't even know the total number of children at risk and another failure of this system is that specialists very often choose not to enter the data in the database because they have too many other duties and don't see the common picture of multisectoral cooperation benefits. Besides, some of the institutions still ask employees to write the same information to the partners in official letters (Ministry of Welfare, Baltic Institute of social Sciences, 2023<sup>5</sup>).

The third case (child C) is about forwarding data. Some information is missing that is an important part of the case. It is due to technical aspects of the program that is passing information to the regional social services. If suspicion about the crime is reported in the data system of Children Hospital by medical personnel, other specialists are supposed to be informed immediately (Berzina, 2023<sup>7</sup>). If the social workers receive the information and then information about child C is given to the other municipality in the region, a lot depends on specialists in the children's protection institutions and social institutions for follow-up and feedback. As mentioned above, databases are partially connected, but not fully. Not in all cases feedback or information is given back to the initial provider automatically. In the case of child C, there were multiple episodes of repeated violence that could have been prevented if there was full and precise information in the databases after the first episode. Child C came back to the hospital in Riga with even more serious wounds. The solution to these cases can only be a human aspect – making phone calls to get more details about the cases and to find out, if more information is available and why it is missing. There are two aspects that can help a child in need - the human aspect and databases that are connected and “talk” clearly

to each other. Human aspect - willingness to help and have an individual approach for each case, updating the database, and checking in with a phone call can solve the case or, at least, make a difference. Unfortunately, we can't always rely on information in the database, at least not yet. Databases should be created to serve people, not the other way around.

### *C. COST-BENEFIT ANALYSIS*

The last example is about how the data about the cost of the state services, especially, the efficiency and cost of criminal justice system work is calculated and compelled.

Cost-benefit analysis (CBA), sometimes also called benefit-cost analysis, is a systematic approach to estimating the strengths and weaknesses of alternatives. It is used to determine options that provide the best approach to achieving benefits while preserving savings in, for example, transactions, activities, and functional business requirements. A CBA may be used to compare completed or potential courses of action, and to estimate or evaluate the value against the cost of a decision, project, or policy. It is commonly used to evaluate government policy investments, what was also the need in Latvia.

It is not a widely known method in Latvia to see the impact of the investments in the development of state services. Nowadays social economic benefits for investments in the public sector are a must. However, the data must be trustful. An especially sensitive issue is cost-benefit analysis in the field of criminal justice and investigation. The first time the method was applied to measure the impact of provided support to the implementation of Barnahus in Latvia. It was done by the OECD in 2023. How long would it take to get a return on investment on the implementation of Barnahus model in Latvia?

What are the ways and challenges to overcome this and still prove the impact of investments to develop Barnahus model? How to get data in this situation when they are so fragmented and should be collected from several institutions, including law enforcement? Conducting the cost-benefit analysis of the implementation of Barnahus model is quite challenging in situations when there is no data available. Can the lack of data be considered data itself? Yes and No. Usually, there are still some of the data available, for example, the average salaries of the employees in law enforcement (police, prosecutors, court experts, judges) and costs of premises and telecommunication. In the case of calculating the cost for the investigation of one case of violence against the child, these data are crucial because the benefit of the model is not only in the best interests of the child-, but also directly connected with the saving of money and time for professionals. In Latvia, no information was fully available about the average length of the case and the costs of the premises and telecommunication. According to the knowledge of the author of this article, no published attempts to measure and calculate the costs to investigate one criminal case from the very beginning to court judgment, followed by rehabilitation were ever made. Overall, modelling many situations and calculating the investments in renovation of premises and equipment for Barnahus, staff costs,

training, and other costs, social economic benefits for children, community and state are paying back. According to the OECD, investing EUR 2.8 million in providing integrated services to child victims or witnesses of abuse and violence can generate EUR 5.5 million in socio-economic benefits over 20 years.

Taking into account the above-mentioned information, the author can fully agree with another conclusion from the research carried out by OECD recently published research is that the uneven quality of data also poses a challenge to the capacity of policymakers and institutions to ensure that child protection and child justice programmes and services are informed by high quality evidence and analysis (OECD, Assessment and recommendations for a child – friendly justice system in Latvia, 2023<sup>3</sup>).

#### CONCLUSIONS

- A. *Fragmented data are not helpful for multisectoral cooperation, neither they help to prevent crime or its investigation;*
- B. *Even with the best designed databases, the human aspect to enter data, to ask and compare information is crucial;*
- C. *Design of the information systems should follow the needs of the client and possibilities to connect them among institutions in one field of work;*
- D. *Resources of IT design and maintaining of services should be merged to serve the needs of the community;*
- E. *No data are also a data and show the lack of policy planning and calculation of the costs to have more efficient state service;*

F. *Cost benefit method is not widely used to measure the impact and effectiveness of law enforcement work to investigate cases of violence against children.*

#### REFERENCES

1. LR Personal Data Processing Law, Latvijas Vēstnesis Nr.132, 04.07.2018. Available: <https://likumi.lv/ta/en/en/id/300099-personal-data-processing-law> (Accessed 02.03.2024)
2. *Latvijas Republikas Tiesībsarga pārbaudes lieta "Par noziedzīgo nodarījumu, kas vērsti pret bērna tikumību un dzimumneatšķirību izmeklēšanu"* Ombudsman's Report about the quality of the Investigation of Cases of Sexual Violence against Children (2021). Available: [https://www.tiesibsargs.lv/uploads/content/gada\\_zinojums\\_versija\\_3\\_2\\_1583476942.pdf](https://www.tiesibsargs.lv/uploads/content/gada_zinojums_versija_3_2_1583476942.pdf) (Accessed 03.03.2024)
3. OECD report on Child Friendly Justice: Implementing Barnahus model (OECD, 2024) Available: <https://www.oecd-ilibrary.org/sites/c607471b-en/index.html?itemId=/content/component/c607471b-en> (Accessed 05.03.2024) <https://doi.org/10.1787/83ab7bf5-en>
4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available: <https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX%3A32016R0679> (Accessed 05.03.2024)
5. *Labklājības ministrijas "Pētījums par vardarbības ģimenē un vardarbības pret bērnu datu monitoringa sistēmas izveidi"* Report about Creation of Monitoring System about Domestic Violence and Violence against Children, Ministry of Welfare, Baltic Institute (2023), Available: <https://www.lm.gov.lv/lv/iepirkums/petijums-par-vardarbibas-gimene-un-vardarbibas-pret-bernu-datu-monitoringa-sistemas-izveidi-2> (Accessed 05.03.2024)
6. UN The Convention on the Rights of the Child. Available: <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child> (Accessed 03.03.2024)
7. I. Bērziņa, "Role of medical practitioners in prevention and investigation of violence against children, and need to strengthen interdisciplinary cooperation in Latvia," Socrates. Rīga Stradiņš University Faculty of Law Electronic Scientific Journal of Law. Volume 2023: Issue 1-26 (October 2023. [Online]. Pages 67-74, and available DOI: <https://doi.org/10.25143/socr.26.2023.2.67-74>

# *Illegal Migration Processes Management In The Light Of The New European Union Pact On Migration And Asylum*

**Jordan Deliversky**

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

**Abstract.** Contemporary border control and migration management policies and practices national wide and within the European Union are usually structured within a framework characterised by a collaboration between public and private interests.

Migration is often related to various risks to national security, including some of them closely related to the regulatory framework. Migration itself, as a complex issue requires the provision of international protection, especially as the pressure to EU external borders provide challenges to border EU countries member states.

This article focuses on specific regulations introduced within the new European union Pact on Migration and Asylum refer to migration management regulation, as its implementation requires exceed of capacities of EU member states countries as well as introduction of specific mechanisms for strengthening cooperation and solidarity in fight against negative consequences for illegal migration.

**Keywords:** *Border control, illegal migration, prevention, regulatory measures.*

## I. INTRODUCTION

The European Union has established a unified system for asylum to ensure protection for individuals escaping persecution or being at risk in their home countries. This system, known as the Common European Asylum System (CEAS), is based on the principles of solidarity and fair treatment across all Member States, ensuring that asylum seekers receive consistent and dignified consideration no matter where they apply within the EU. The bases of the Common European Asylum System are formed by several legal instruments and include a specific body established to harmonize asylum procedures and standards across the EU. This includes directives and regulations that outline the

procedures for asylum applications, establish common standards for the treatment and reception of asylum seekers, and determine the Member State responsible for processing an asylum application. The European Union Agency for Asylum supports the implementation of these standards, offering operational and technical assistance to Member States [1].

The bases of evolution of Common European Asylum System reflects the EU's response to fluctuating migration pressures and aims at enhancing the system's efficiency and fairness. Reforms have been introduced to streamline processes, promote equitable responsibility sharing among Member States, and foster stronger cooperation within the European Union and also with non-EU countries. These efforts are included in initiatives like the New Pact on Migration and Asylum, which seeks to rebalance the principles of responsibility and solidarity within the EU's asylum policy.

As a Member State country of the European Union, Bulgaria is actively involved in the implementation of the main legislative acts on migration in the EU, including the Asylum procedures directive, the reception conditions directive, the qualification directive and the Dublin regulation determining which Member State is responsible for examining a given asylum application. The country has introduced CEAS's directives and regulations into its national legal framework, adhering to the shared objectives and standards set by the EU for asylum procedures and refugee protection. This alignment ensures that asylum seekers in Bulgaria are subject to the same levels of protection and procedural fairness as in other EU countries [2], [3].

The ongoing developments within the Common European Asylum System underline the EU's commitment

*Print ISSN 1691-5402*

*Online ISSN 2256-070X*

<https://doi.org/10.17770/etr2024vol4.8239>

© 2024 Jordan Deliversky. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

to refining its asylum system. These efforts aim to address contemporary challenges and ensure that the rights and needs of asylum seekers and refugees are met with the required respect and safety across the European Union [4].

The focus of researching and presenting the issue of illegal migration management processes in the light of the New European Union Pact on Migration and Asylum provides bases for analyses of the Pact presenting specific mechanisms for managing illegal unauthorised migration. By conducting a thorough assessment such research is of capability to shed light on the practical outcomes of the EU's migration policies. It is a contributing valuable perspective to enhance future policy migration management framework within the European Union especially upon the aspect of obligations towards migrants and asylum seekers.

## II. MATERIALS AND METHODS

The European Union's recent provisions of the New Pact on Migration and Asylum represents a significant evolution in its approach to managing migration and asylum requests. Enacted to offer a more equitable, effective, and sustainable system, this framework, finalized in late 2023, emphasizes a harmonized strategy focused on human rights, shared responsibility, and solidarity among EU countries.

At its core, the pact regulates several legislative and policy changes aimed at enhancing the EU's migration and asylum processes. Key innovations include a standardized screening process for arrivals from outside the EU to bolster the security of the Schengen zone, the creation of an upgraded Eurodac database for improved monitoring of movements, streamlined procedures for asylum and returns, a novel mechanism to distribute the responsibility of asylum applications more evenly among Member States, and preparations for handling future migration crises efficiently [5], [6].

Prior initiatives under the pact have laid the groundwork for improved crisis management, search and rescue operations, and the establishment of the European Union Agency for Asylum, which succeeds and expands upon the European Asylum Support Office's mandate. These steps, alongside the appointment of an EU Return Coordinator and the launch of a Voluntary Solidarity Mechanism, signify the EU's commitment to a cooperative and coordinated approach to migration challenges [7].

This landmark pact aims to reconcile the diverse interests and capacities of EU member states in handling migration and asylum issues, set against a backdrop of political and social complexities. The successful implementation of this comprehensive strategy hinges on member states' adherence to its principles, effective execution of its policies, and the adaptability of the EU to future challenges in migration management.

The Pact's impact on future EU migration policy remains to be seen, with its ultimate success depending on a bases of solidarity, protection of human rights and efficient management of migration and asylum procedures across the EU.

An in-depth policy analyses of the European Union's New Pact on Migration and Asylum illustrates a complex

strategy aimed at revising the EU's approach to managing migration and asylum requests to better confront modern challenges. The pact, officially endorsed by both the European Parliament and the Council in late 2023 after its initial proposal in 2020, strives to deliver a harmonized and enduring framework that emphasizes human rights, equitable responsibility distribution, and enhanced procedural efficiencies for migration and asylum within the EU [8].

The pact lays out several specific legislative and policy initiatives designed to refine the EU's asylum and migration framework. These include elements related to:

- Focusing on the prompt identification and security assessment of non-EU nationals upon entry, aiming to solidify the security across Europe and the Schengen zone.
- Steps to improvement and higher efficiency of the use of asylum fingerprint database for better tracking and managing migration activities.

## III. RESULTS AND DISCUSSION

The efficacy of the implementation of the European Union's Pact on Migration and Asylum new solidarity mechanism is crucial for its overall success. This approach aims at equitable distribution of migration-related responsibilities across the EU, addressing longstanding points of contention. The mechanism's impact will largely depend on the collaborative spirit and mutual support among EU countries.

The introduction of the Pact represents a reform effort within the EU's approach to migration and asylum, necessitating a thorough evaluation against global human rights standards, including key international treaties and conventions [9]. Special attention has to be paid to how the new EU Pact addressing the needs of vulnerable migrants and asylum seekers. The effectiveness of the Pact's provisions for identifying and protecting vulnerable individuals, including integration and protection measures, is critical for evaluating its human rights impact [10].

It is important for visibility to be provided for understanding how the New Pact's initiatives result to ensuring equitable asylum procedures, strengthen border security, and promoting Member State solidarity comport with established specific measures related to applying human rights protection mechanism.

Analyzing Bulgaria's approach to the European Union's Migration and Asylum Pact, along with its domestic legal development, is easy to provide insights into the country's strategic positioning and operational effectiveness within the EU framework. Due to the geographic extend and the position where the county is situated within the EU's borders, Bulgaria is important factor in managing external borders and handling migrant inflows [11]. Bulgaria's role in EU solidarity mechanisms and partnerships with third countries is critical for distributing asylum responsibilities and managing repatriations. This involves assessing Bulgaria's participation in EU-wide redistribution initiatives and its agreements with non-EU countries on migration management.

Identifying obstacles to the effective implementation of the new regulatory steps in the light of the New European Union's Pact on Migration and Asylum, as specifically the level of implementation in Bulgaria is crucial for enhancing Bulgaria's migration management systems.

The policy of the Republic of Bulgaria in the field of migration, integration and granting of asylum is based on the national interests of the country and the coordinated approach of the EU member states and the institutions operating within the framework of the European Community, as well as in accordance to the principles of international law - including the principle of rule of law and the principle of protection of human rights.

Bulgaria has adopted National Migration Strategy from 2021 to 2025 which is being implemented and is currently applied. In administrative context, the regulation of migration processes, in regards to the implementation of activities by the executive power, places the Ministry of Internal Affairs - via the Directorate of Migration - at the focus of significant importance. This applies with particular accuracy in regards to the implementation of administrative control rules over the residence of foreigners in the Republic of Bulgaria and activities directed to countering illegal migration on the territory of the country. The Directorate of Migration is also engaged in administrative services to citizens of the European Union, citizens of countries - parties to the Agreement on the European Economic Area, citizens of the Swiss Confederation, as well as their family members [12], [13].

The resultativeness in counteraction of illegal migration and detecting illegal human trafficking activities is being specifically affected by the conditions and the mechanism by which border control is carried out when entering and leaving the territory of the country. Specific elements and main factors, related to activities of the "Border Control" Directorate provides the bases for setting the structure at the Ministry of Interior, as the responsible national competent authority for the implementation of the EU rules and procedures on return of non- EU nationals who are staying on the territory of the county not based on legal grounds [14].

The current national legislative framework in the field of migration has been under dynamic development on the one hand, following the guidelines set by the European Union, as on the other hand, providing the ability to respond to the national interest [15]. The development in policies and regulatory processes related to the adoption of legislative acts at a European level is being guided and fulfilled by specialists and by experts in the field of migration and asylum. These actions are being reflected in legislative initiatives undertaken by the competent authorities responsible for implementing and conducting migration policy.

Last but not least, the legislation is to be updated to meet the changing needs within the Bulgarian society, so that it responds to national requirements, synchronized with regional strategies and international policies, especially in the context of detecting and countering illegal migration.

#### IV. CONCLUSION

The European Union's recent provisions of the New Pact on Migration and Asylum represent a significant evolution in its approach to managing migration and asylum requests. Enacted to offer a more equitable, effective, and sustainable system, this framework, finalized in late 2023, emphasizes a harmonized strategy focused on human rights, shared responsibility, and solidarity among EU countries. The European Union's Pact on Migration and Asylum is a landmark initiative attempting to navigate the complex realm of migration and asylum with a more cohesive and humane approach.

For Bulgaria, as for other European Union member states the Pact on Migration and Asylum address challenges as to the migration management system introducing significant focus on resilient and alignment with human rights grounds and standards, as balancing responsibilities of frontline EU Member State countries, which are also external border countries.

At the core of the Pact has been focused the mechanism of solidarity, offering Member States to apply various mechanisms to support one another especially in regards to intense migration pressure without mandating the relocation of migrants.

The actual success of this Pact will largely hinge on the collective efforts of EU Member States to implement its guidelines faithfully, ensuring a balance is struck between procedural efficiencies and the safeguarding of human and asylum seekers' rights. Continuous monitoring and adjustment will be necessary to ensure the pact meets its goals while adapting to the global migration landscape's evolving nature

#### REFERENCES

- [1] Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council establishing a common procedure for international protection in the Union and repealing Directive 2013/32/EU, Feb. 2024.
- [2] 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, OJ L180, 29.6.2013, p. 60
- [3] European Commission, The Common European Asylum System (CEAS) factsheet. [Online]. Available at: [https://home-affairs.ec.europa.eu/system/files/2016-12/factsheet\\_-\\_the\\_common\\_european\\_asylum\\_system\\_en.pdf](https://home-affairs.ec.europa.eu/system/files/2016-12/factsheet_-_the_common_european_asylum_system_en.pdf) [Accessed March 16, 2024]
- [4] European Union Agency for Asylum, Asylum Report 2023. [Online]. Available at: <https://euaa.europa.eu/asylum-report-2023> [Accessed March 16, 2024]
- [5] Zahariev, Martin, Radoslava Makshutova; GDPR Implementation Series: Bulgaria; European Data Protection Law Review (EPDL), Berlin, 2020, Lexxion Verlag, Volume 6, Issue 3, pp. 424-432, ISSN 2364-2831
- [6] European Policy Centre, Navigating the New Pact on Migration and Asylum in the Shadow of Non-Europe, Jan. 2024. [Online]. Available at: [https://www.epc.eu/content/PDF/2024/Non-Europe\\_migration\\_policy\\_DP\\_v2.pdf](https://www.epc.eu/content/PDF/2024/Non-Europe_migration_policy_DP_v2.pdf) [Accessed March 16, 2024]
- [7] International Legal Research Group on Migration, The European Law Students' Association Report, March 2018
- [8] European Policy Centre, The Common European Asylum System, 2020. [Online]. Available at: [https://www.epc.eu/content/publications/7\\_CEAS.pdf](https://www.epc.eu/content/publications/7_CEAS.pdf) [Accessed March 16, 2024]
- [9] European Court of Auditors, EU Migrant return policy – cooperation with third countries on readmission, July 2020. [Online]. Available at:

[https://www.eca.europa.eu/lists/ecadocuments/ap20\\_07/ap\\_migrant\\_return\\_policy\\_en.pdf](https://www.eca.europa.eu/lists/ecadocuments/ap20_07/ap_migrant_return_policy_en.pdf) [Accessed March 16, 2024]

- [10] European Commission, A humane and effective return and readmission policy, 2023. [Online]. Available at: [https://home-affairs.ec.europa.eu/policies/migration-and-asylum/irregular-migration-and-return/humane-and-effective-return-and-readmission-policy\\_en](https://home-affairs.ec.europa.eu/policies/migration-and-asylum/irregular-migration-and-return/humane-and-effective-return-and-readmission-policy_en) [Accessed March 16, 2024]
- [11] Neikova, Maria., The concept of "National security" - modern aspects [in Bulgarian], Legal Collection, Burgas Free University, Center for Legal Studies, Volume XXIV, 2017, pp. 11-18.
- [12] National Migration Strategy of the Republic of Bulgaria 2021-2025, Council of Ministers' Decision No. 256 of 25.03.2021.
- [13] Bulgarian Helsinki Committee, Asylum Information Database, Country report on Bulgaria, 2022. [Online]. Available at: <https://www.bhc.org.uk/aiad/country-reports/bulgaria>
- [14] European Union, Together Against Trafficking in Human Beings, Feb. 2024. [Online]. [https://home-affairs.ec.europa.eu/policies/internal-security/organised-crime-and-human-trafficking/together-against-trafficking-human-beings\\_en](https://home-affairs.ec.europa.eu/policies/internal-security/organised-crime-and-human-trafficking/together-against-trafficking-human-beings_en) [Accessed March 16, 2024]
- [15] Zahariev, Martin, Legal guarantees for the security of personal data processed by the competent authorities for police and criminal activities [in Bulgarian], Proceedings book, National Scientific Conference with International Participation „Security and Defence“, Academic publishing house „Za bukвите – O pismeneh“, Sofia, 2023, p. 492-506, ISBN 978-619-185-593-3.



# *Applying Artificial Intelligence for improving Situational awareness and Threat monitoring at sea as key factor for success in Naval operation*

**Todor Dimitrov**  
Command and Staff Faculty  
Rakovski National Defence College  
Sofia, Bulgaria  
t.d.dimitrov@rncd.bg

**Abstract.** The vast and dynamic maritime domain demands constant observance and accurate information for successful naval operations. However, traditional methods struggle to keep pace with the ever-increasing complexity and data overflow. The paper explores how Artificial Intelligence (AI) presents a transformative opportunity, significantly impacting naval operation by enhancing Situational awareness (SA) and Threat monitoring (TM). It is analyzed the impact of AI across three key areas: enhanced data processing and analysis, improved anomaly detection and predictive capabilities, and real-time decision support. By analyzing key principles, tactics, and procedures for AI implementation, it is explored the process how these capabilities can convert into practical applications and benefits. Examples like AI-powered maritime surveillance and predictive systems for naval assets demonstrate solid benefits of this technological progress. Additionally, in the paper are envisioned future operational scenarios where AI-driven autonomous systems and dynamic route optimization become commonplace. The analysis demonstrates how AI can be a critical factor in moving naval operations into a new era of efficiency and proactive threat management. However, responsible development and ethical considerations remain of paramount importance.

**Keywords:** *Artificial Intelligence, Naval operation, Situational awareness, Threat monitoring.*

## I. INTRODUCTION

Situational awareness (SA) and threat monitoring (TM) are critical components of naval operations, playing a pivotal role in maintaining security, operational effectiveness and strategic advantage at sea. Their importance can be defined across several key dimensions like support of informed decision-making and strategic planning, understanding the real-time status of the operational environment, including the location, capabilities and intentions of both friendly and potential adversarial forces. Effective TM enables early detection of potential threats and what is more it is crucial for timely

response, allowing naval forces to mitigate threats before they can affect maritime operations or escalate into larger conflicts [1]. There are several operational gaps in traditional SA and TM approaches in naval operations and the application of Artificial Intelligence (AI) - driven tools is one of the successful approaches to improve these processes.

## II. MATERIALS AND METHODS

### A. *Situational awareness and Threat monitoring as a Key Factors for Naval Operation*

Situational awareness and threat monitoring are foundational to the success of naval operations. They enhance decision-making, ensure force protection, enable effective threat response and provide a strategic advantage, thereby playing a vital role in maintaining maritime security and stability [2]. These two pivotal elements in naval operations are supporting the safety, efficiency and effectiveness of maritime forces. These components are crucial for several reasons: Situational awareness is Enhancing Decision-Making as it provides naval commanders and personnel with a comprehensive understanding of the environment in which they operate. This includes knowledge of the location, status and intentions of both friendly and adversarial forces, as well as relevant civilian entities at sea. Accurate and timely information allows for informed decision-making, enabling strategic planning and tactical responses to dynamic situations [1]. At the same time Threat Detection (Threat monitoring) is essential for the early detection of potential threats, ranging from conventional military assets like warships, submarines and mines to asymmetric threats such as piracy, terrorism, smuggling and illegal fishing. Early detection enables naval forces to assess threats accurately and initiate appropriate countermeasures (Threat Response), thereby mitigating risks and preventing escalation. It allows commanders to make tactical decisions that are critical for mission success. Moreover, maintaining

Print ISSN 1691-5402  
Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8224>

© 2024 Todor Dimitrov. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

SA is key to protecting naval assets and personnel (Force Protection) from both military and non-military threats. This includes not only direct attacks but also environmental hazards and navigational risks. Effective monitoring and awareness mechanisms ensure that forces remain alert and prepared to respond to any incident, ensuring the safety and integrity of naval operations. In an era of joint and combined operations, situational awareness facilitates interoperability and coordination among allied forces in multidimensional battlespace [3]. Sharing a common operational picture enhances the ability of multinational forces to operate cohesively, coordinate actions and achieve shared objectives, thereby amplifying collective defense capabilities [4]. Furthermore, superior situational awareness provides a strategic advantage by enabling naval forces to anticipate adversary actions, exploit vulnerabilities and maneuver effectively in the maritime domain. This advantage is critical in both conventional warfare scenarios and in countering non-traditional threats. In addition to its military applications, situational awareness is crucial for crisis management and humanitarian assistance operations. It enables naval forces to quickly assess situations, such as natural disasters or maritime accidents and provide timely and effective aid, thereby saving lives and mitigating the impact of crises. Maintaining high SA and demonstrating the capability to monitor and respond to threats can serve as a deterrent to potential adversaries. It signals readiness and the ability to project power when necessary, contributing to stability and peace in international waters. To sum it up, SA and TM are indispensable for modern naval operations, enabling forces to navigate the complexities of the maritime environment effectively, respond to emerging threats promptly and conduct operations that support national and international security objectives [5].

#### *B. Operational gaps in traditional approaches to Situational Awareness and Threat Monitoring in Naval operations*

There are several challenges in traditional approaches to SA and TM in naval operations, driven by the complexity of the maritime environment, technological limitations and evolving threats. First of all, is Data Overload when during Naval operations is generated vast amounts of data from various sources, including radar, sonar, satellites and intelligence reports. The complete volume of information can overwhelm traditional analysis methods, leading to delays in processing and potential gaps in SA. Naval forces often rely on a variety of legacy systems and sensors that may not be fully compatible with each other. Integrating data from these disparate sources into a coherent operational picture is a significant challenge, obstructing effective decision-making. Moreover, the maritime domain is by its nature dynamic, with rapidly changing conditions and high degrees of uncertainty. The physical environment of the sea, including weather conditions, underwater geography and the vastness of the ocean, poses natural challenges to monitoring and awareness. Traditional methods may be limited in their ability to account for these factors effectively and may struggle to adapt quickly to new information or unexpected situations, potentially compromising SA [6]. Also, while traditional systems can collect and store data, they may lack the capability for real-time analysis and interpretation. This

delay can be critical in fast-moving situations where immediate responses are required to mitigate threats. At the same time, as naval operations become increasingly dependent on digital systems, they become more vulnerable to cyber threats. Traditional security measures may not be sufficient to protect against sophisticated cyber attacks aimed at disrupting SA and command and control systems. What is more, Naval forces face a broad spectrum of threats, including asymmetric tactics employed by non-state actors, piracy, terrorism and cyber warfare. Traditional approaches may not be designed to detect or respond effectively to these unconventional threats. Maintaining comprehensive SA requires significant resources, including advanced sensors, surveillance assets and skilled personnel. Budgetary and operational constraints can limit the ability of naval forces to deploy these resources effectively. Also, Joint and coalition operations are integral to modern naval strategy, demanding interoperability among diverse forces [3]. Achieving integrated communication and data sharing between different countries and branches of the military remains a challenge, affecting SA. Reliance on manual processes and human interpretation of data can introduce errors and biases into SA and TM. Fatigue, cognitive overload and the limitations of human decision-making under stress can further impact the effectiveness of traditional approaches. Addressing these challenges requires innovative solutions that use advance in technology, such as AI, machine learning and automated systems, to enhance the speed, accuracy and adaptability of SA and TM in naval operations.

#### *C. Applying Artificial Intelligence in Naval operation*

In recent years, modern technologies have developed rapidly, which in turn also greatly affects naval activities. AI technologies have significantly enhanced SA and TM in naval operations by providing advanced capabilities for data analysis, decision support and operational efficiency. AI-driven tactics significantly enhance SA in naval operations by using advanced computational techniques like predictive analytics, pattern recognition, machine learning and more. These tactics enable forces to interpret complex data, anticipate future scenarios and make informed decisions promptly. There are a few key AI-driven tactics for enhanced SA like: Predictive Analysis, Pattern Recognition, Machine Learning and Deep Learning, Natural Language Processing (NLP), Sensor Fusion, Decision Support Systems, Cybersecurity, Human-AI Collaboration, etc. After analyzing of the researched topic, the following key factors can be summarized for AI's contribution in Naval operation:

##### *a) Data Fusion and Analysis*

AI algorithms can integrate, process and analyses vast amounts of data from sensor networks with diverse sources, including satellites, radar, sonar, unmanned and ship-based sensors, like automatic identification system - AIS. AI also integrates data from above mentioned sensor networks and Internet of Things (IoT) devices deployed on naval assets and maritime infrastructure. This integration facilitates the continuous monitoring of operational environments and asset conditions. By employing algorithms that can process and fuse data in real-time, AI

provides a comprehensive and integrated operational picture, enabling more accurate situational awareness of both the physical and electronic environments. This capability enhances SA, allowing naval forces to monitor vast ocean areas efficiently and detect subtle changes or threats that might be overlooked by human operators.

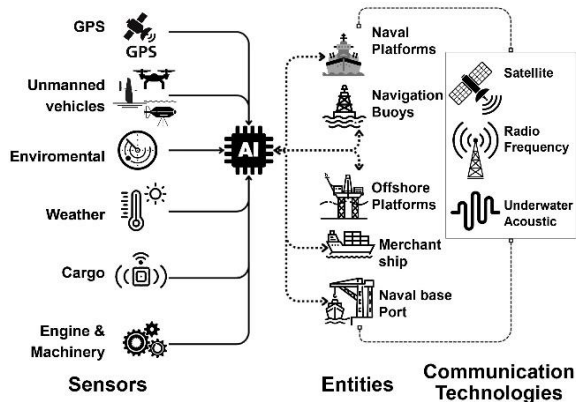


Fig. 1. Model of AI-driven Data Fusion and communication lines

#### b) Automated Threat Detection

Machine learning and pattern recognition models, a subset of AI, are trained to detect anomalies, classify objects and identify potential threats with high accuracy. These models can differentiate between civilian and military assets, detect unusual behaviour indicative of piracy or terrorism and identify environmental hazards, significantly reducing the response time to potential threats, including asymmetric ones like unmanned aerial vehicles (UAVs), mines or swarms of small boats. Machine learning models can learn from historical data to identify patterns associated with different types of threats, improving accuracy and reducing false positives. AI models are trained to recognize normal patterns of maritime traffic and environmental conditions. Any deviation from these patterns (Anomaly Detection), such as an unusual navigational route or speed, can be flagged as a potential threat, triggering further analysis or immediate action. AI can classify objects based on their "signatures" or unique characteristics captured by sensors (Signature Recognition). For example, the acoustic signature of a submarine or the radar cross-section of a surface vessel can be used to identify and classify potential threats. Regarding Target Identification and Classification could be used AI systems trained on vast amounts of imagery and sensor data that can automatically identify and classify contacts as civilian, commercial or military assets, significantly speeding up the decision-making process. What is more, Adaptive Learning Systems continually learn from new data, improving their accuracy and effectiveness over time. This capability is crucial for adapting to evolving sea threats and operational environments. Machine Learning and Deep Learning could support Image and Voice Recognition. Deep learning models are particularly effective in image and voice recognition tasks, useful for ISR (Intelligence, Surveillance, Reconnaissance) missions at sea. They can process satellite imagery or intercept communications to gather actionable information. For example, to identify specific vessel types, recognize patterns indicative of hostile intent and even detect concealed or camouflaged objects. On the other hand, using

Natural Language Processing (NLP) techniques can automatically analyze vast quantities of text data from news, social media and other open sources to gather information (Open Source Intelligence - OSINT), identify potential threats and understand sentiment and intentions.

#### c) Predictive Analysis

AI leverages historical data and predictive analytics to forecast future threats and trends. Machine learning algorithms excel at detecting anomalies in vast sea datasets, identifying unusual ship movements, electronic signatures or communication patterns that could indicate threats like piracy, smuggling or enemy activity. Predictive analytics can identify patterns that precede attacks or aggressive maneuvers, allowing preemptive action. This capability allows naval forces to anticipate adversarial moves, plan defensive strategies and position assets strategically, enhancing preparedness and strategic decision-making. For naval operation this can be a game-changer, enabling proactive rather than reactive approaches, allocating resources more effectively and preparing for potential security challenges [7].

#### d) Enhanced Decision-Making

AI technologies have significantly improved the efficiency of naval operations by automating the analysis of sensor data, leading to quicker and more accurate decision-making processes. AI supports decision-making by providing actionable insights, recommendations and automated decision aids [8]. By analyzing complex scenarios and considering numerous variables, AI systems can suggest optimal courses of action, helping commanders make informed decisions quickly under various conditions [8].

#### e) Improved Surveillance and Reconnaissance

AI is a key enabler for unmanned systems - aerial, underwater and surface vehicles (UAVs, UUVs, USVs) and enhance surveillance and reconnaissance missions. AI algorithms enable these assets to navigate autonomously, avoid obstacles and identify areas of interest for further investigation, extending the reach, duration and effectiveness of naval surveillance efforts. These systems can conduct data gathering and even perform initial threat assessments autonomously. In the littoral zone, unmanned systems operated by AI can operate stealthily, avoiding detection while providing persistent surveillance. This is particularly beneficial for monitoring in politically sensitive areas or environments where human deployment is risky or infeasible. AI enables the real-time processing of sensor data, crucial for timely threat detection. This capability allows naval forces to react promptly to potential threats, enhancing maritime security and operational readiness. In this way they reduce risks to human life and increase the areas covered.

#### f) Cybersecurity and Information Warfare

In the digital and information age, SA extends to cyberspace and the electromagnetic spectrum. Monitoring communications, detecting electronic signatures and understanding the informational environment are critical for maintaining an operational advantage and ensuring cybersecurity. In the domain of cybersecurity, AI tools monitor network traffic and detect anomalies that could indicate cyber threats. AI-driven cybersecurity measures

are essential for protecting critical naval communication and operational systems from hacking, espionage and sabotage. That tools strengthen cybersecurity measures, detecting and neutralizing threats more efficiently [9].

g) Logistics Optimization

AI also plays a crucial role in optimizing the allocation of resources, including personnel, ships and surveillance assets. It can predict equipment failures before they occur by analyzing data from sensors and maintenance logs, enabling preventative maintenance and reducing downtime. Through sophisticated modelling and simulation, AI systems can recommend the most efficient deployment of naval resources, optimize supply chains and logistics, ensuring maximum coverage and operational effectiveness [10].

h) Training and Simulation

AI-powered simulations and virtual training environments offer realistic, scalable training opportunities for naval personnel. These tools can simulate a wide range of scenarios, from routine operations to complex combat situations, enhancing readiness and operational skills without the risks and costs associated with live training exercises. These tools support continuous learning and skills development, ensuring that forces are prepared for any challenge.

To sum it up, AI-driven technologies significantly contribute to SA and TM in naval operations by providing comprehensive data analysis, enhancing threat detection and prediction, supporting decision-making and optimizing resource allocation. As AI technology continues to evolve, its role in naval operations is expected to grow, offering even more sophisticated tools for ensuring maritime security and operational success.

D. PROCEDURES FOR INTEGRATING AI TOOLS WITH NAVAL OPERATION PROTOCOLS

Integrating AI-driven tools into naval operation protocols involves a series of methodical procedures

designed to ensure that AI technologies enhance

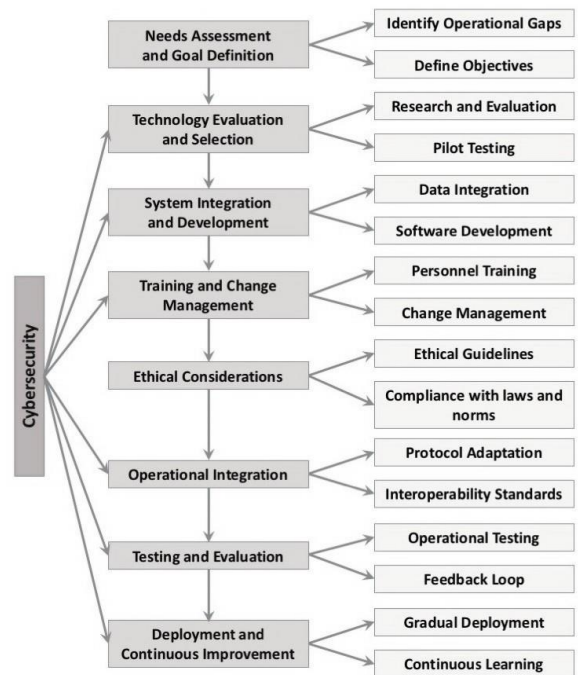


Fig. 2. Structured approach for integrating AI tools within Naval operation protocols

operational capabilities without compromising security or effectiveness. These procedures typically include technological, operational and organizational dimensions, ensuring a trouble-free and effective integration. Here's a structured approach for integrating AI tools within naval operation protocols "Fig. 2": First of all, should be defined Needs Assessment and Goal Definition for such an operation. For that purpose it is needed to be Identified Operational Gaps. It is conducted a thorough assessment to identify areas within naval operations where AI can offer significant improvements, such as decision support, threat detection or logistics management. To define objectives it is needed clearly to define what the integration aims to achieve, including specific performance metrics or capabilities to be enhanced by AI. Secondly, Technology Evaluation and Selection should be done. It is done by researching and evaluating available AI technologies and tools that meet identified needs, taking into account factors such as compatibility with existing systems, scalability and cybersecurity implications. After that, there are Implemented pilot projects or trials (Pilot Testing) with selected AI tools to assess their effectiveness, usability and integration challenges in a controlled environment. System integration and development of the integrating software takes place next. AI tools need to be able to access and process data from existing naval data sources and sensor systems, implementing necessary interfaces or data processing pipelines. Artificial intelligence software is developed or customized to align with specific protocols and requirements for naval operations, incorporating user feedback from pilot testing. In addition, it is necessary to train the personnel and to manage changes in the system. It is important to train staff on the use and interpretation of AI tools, with a focus on how these tools develop existing protocols and decision-making processes. Change management strategies are implemented to address potential resistance and ensure smooth adoption of AI

technologies within the organizational culture. Cybersecurity protocols need to be put in place next. Robust measures are integrated to protect AI systems from potential threats and vulnerabilities, thereby ensuring the integrity of naval operations. Establishing ethical guidelines for the use of AI, especially for decision-making in combat scenarios, ensuring compliance with international laws and norms is also a priority [5]. Existing naval operational protocols need to be adapted to incorporate AI-driven insights and recommendations, including updates to command and control procedures. It is critical that AI tools adhere to interoperability standards for joint operations with allied forces, facilitating seamless collaboration. It is also important to conduct extensive testing under realistic operational conditions to evaluate the performance and impact of AI tools on naval operations. Feedback Loop is needed to establish mechanisms for continuous feedback from users to identify areas for improvement and upgrade AI tools accordingly. Gradual Implementation of AI tools into naval operations should be phased in, monitoring effectiveness and addressing issues as they arise. Next, it is important to use AI's capabilities to continuous learning from new data and experience, updating models and algorithms to improve performance over time. Once AI systems are deployed, it is necessary to organise Current Monitoring systems to track the effectiveness and impact of AI tools on naval operations. This will ensure that they continue to meet operational needs. It is also important to plan regular maintenance and updates for AI systems, taking into account advances in AI technology and adapting to evolving operational requirements. Integrating AI tools into naval operation protocols is a dynamic and ongoing process, requiring close collaboration between technology providers, operational personnel and decision-makers. By following these structured procedures, naval forces can effectively use the potential of AI to enhance SA, decision-making and operational efficiency.

### III. RESULTS AND DISCUSSION

#### A. Model of Situational Awareness of AI-assisted Naval operation

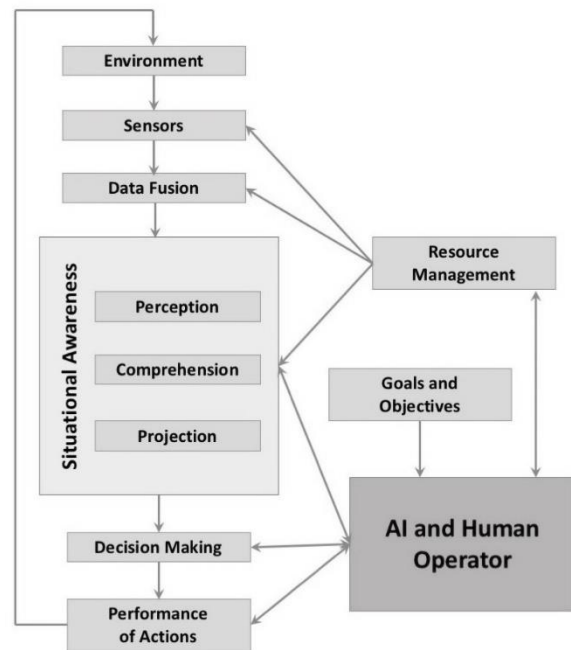


Fig. 3. Model of SA of AI-assisted Naval operation.

The integration of AI with existing naval operation frameworks represents a critical evolution in maritime defense capabilities. The algorithm of this operation is complex, involving technological, operational, and organizational adjustments. AI can enhance sensor fusion capabilities, integrating data from diverse sources such as radar, sonar, satellites, and intelligence reports to provide a comprehensive operational picture. This integration supports better decision-making by offering real-time, enhanced SA [11]. The first stage of attaining situational awareness is the perception of the status and attributes of the entities in the environment. For instance, a ship commander needs to differentiate important entities in the environment such as other ship, shore and warning buoy along with their relevant characteristics. The second stage of SA is the comprehension of the situation, which is based on the integration of disconnected level 1 SA elements. This is understanding of entities in the surroundings, in particular when integrated together, in connection to the operator's objectives. The third level of SA – Projection relates to the ability to project the future actions of entities in the environment at least in the near term. This is prediction or estimation of the status of entities in the surroundings in future.

Many naval operations rely on legacy systems with significant investments in infrastructure and training. AI technologies can be integrated into these systems through software upgrades and the addition of AI-driven analytics modules, thereby enhancing their capabilities without necessitating complete overhauls. AI can facilitate the shift towards more network-centric operations, where distributed sensor networks and platforms share data seamlessly across various assets. AI algorithms can process this data collectively, enabling more cohesive and informed responses to threats. At the organizational level, AI can

assist in strategic decision-making by providing comprehensive analyses of potential courses of action, including their likely outcomes and risks. This support helps commanders make more informed decisions, balancing tactical objectives with strategic goals. Integrating AI into naval operation frameworks is a multidimensional effort that requires careful planning, coordination, and adaptation. By addressing technological, operational, and organizational aspects, naval forces can use AI to enhance their capabilities, maintain strategic advantages, and address the evolving challenges of maritime security.

#### *B. Future development of Artificial Intelligence for improving Situational Awareness and Threat Monitoring at sea*

As these technologies continue to evolve, future developments could include more sophisticated sensor fusion algorithms, the integration of quantum computing for faster data processing, and the creation of more resilient Artificial neural networks (ANNs) capable of operating in adversarial conditions or with limited data [12]. The ongoing advancement in AI and machine learning promises to further enhance naval TM, ensuring that naval forces can effectively counter both conventional and asymmetric threats in increasingly contested maritime environments. It also should be account that potential adversaries are also beginning to use AI technologies, researching competitive AI tactics and developing countermeasures will be critical to maintaining strategic advantages. Future development will enhance AI's ability to support decision-making in environments with incomplete or ambiguous information represents a critical research area, especially for complex naval operations where uncertainty is a constant factor. Also, it will be broadening Integration of AI with existing Naval systems. Research into seamless integration methods for AI technologies with existing naval platforms and systems can ensure that advancements are more readily adopted and operationalized. Will be putted more efforts in developing frameworks and guidelines for the ethical use of AI in military contexts, including transparency, accountability and compliance with international laws, will be increasingly important. Exploring optimal ways for AI systems and human operators to interact and collaborate can enhance SA and operational effectiveness [10]. This includes human-machine interfaces that facilitate intuitive decision-making and control. In that way can be presented AI-generated insights in an understandable and actionable manner enables effective human-AI collaboration, ensuring that commanders can use AI recommendations without being overwhelmed by data. Collaboration between AI systems and human operators will keep the direction ensuring that AI supports rather than replaces human judgment. Also, will be increased Resilience against AI failures. Investigating methods to enhance the resilience of AI systems against failures or manipulations, ensure that naval operations can maintain integrity even when AI systems are compromised [10]. Will proceed efforts in utilizing AI to develop more sophisticated simulation environments for training naval personnel in complex, multi-threat scenarios can improve preparedness and adaptability. Regarding TM will be expanded the use of AI in monitoring and responding to environmental threats to maritime operations, such as climate change

impacts, pollution and natural disasters. AI can also be applied to optimize naval supply chains and logistics, ensuring the efficient allocation of resources and materials in support of operational readiness. These directions underscore the dynamic nature of AI research within the naval domain, highlighting both the potential and the challenges of using AI to enhance maritime security and operational capabilities [7]. The continuous evolution of AI technologies promises to further transform naval operations, making ongoing research and development a critical priority.

Looking ahead, the potential of AI in naval operations includes further advancements in quantum computing, enhanced human-machine teaming and the development of AI strategies that can dynamically adapt to changing operational environments. As AI technology evolves, its role in naval operations is set to expand, offering unprecedented opportunities to enhance maritime security, operational efficiency and strategic advantage.

#### *C. Ethical and Legal considerations*

Using AI in naval operations involves a complex interaction of ethical and legal considerations. As AI systems become more integrated into defense mechanisms and operations, their potential to enhance security and operational efficiency is significant. However, these developments also raise important concerns that must be addressed to ensure responsible use. AI's role in decision-making processes, especially in critical scenarios involving potential threats, raises ethical questions about autonomy. The extent to which AI should be allowed to make decisions, particularly those involving lethal force, is a major concern. The principles of human oversight and control are paramount to ensure that decisions are made ethically and responsibly [8]. Moreover, AI systems are only as objective as the data they are trained on. There's a risk of continuing or even intensifying existing biases if the training data is not carefully selected. In naval operations, this could lead to unfair targeting or the overlooking of threats due to biased algorithms. Ensuring fairness and avoiding bias is essential for ethical AI use. Another important concern regard Transparency and Explainability. AI systems, particularly those based on complex algorithms like deep learning, often operate as "black boxes," making it difficult to understand how they arrive at certain decisions. In the context of naval operations, the lack of transparency and explainability can be problematic, especially when decisions need to be justified or reviewed. Ethical AI requires mechanisms to make its decision-making processes more interpretable. Also, when AI systems are involved in critical operations, determining accountability for decisions becomes challenging. In cases where AI leads to unintended consequences, it's essential to have clear frameworks for accountability and responsibility, ensuring that human operators remain ultimately responsible for decisions made with AI assistance.

The use of AI in naval operations must comply with international laws and norms. This includes principles of distinction, proportionality and necessity, which must guide the deployment and actions of AI systems. AI systems used in naval operations must operate within the established rules of engagement (ROE), which are

designed to regulate the use of force. Ensuring that AI systems can accurately interpret and apply ROE in complex, rapidly evolving situations is a significant legal challenge. The use of AI for surveillance and TM can raise sensitive issues regarding sovereignty and the rights of passage through territorial waters. AI systems must be designed to respect national borders and adhere to international agreements regarding maritime navigation. Also, it is a legal and ethical requirement to balance security needs with respect for privacy.

Developing robust frameworks for governance, oversight and accountability will help ensure that AI technologies are used in ways that are both legally obedient and ethically complete.

#### IV. CONCLUSION

Implementing of AI-driven tactics requires careful integration into existing naval operation frameworks, ensuring that AI systems complement and enhance human decision-making processes. By doing so, naval forces can significantly improve their SA, operational effectiveness and strategic agility in responding to both conventional and asymmetric threats.

AI's application in surveillance and reconnaissance missions at sea and in the littoral zone significantly enhances naval capabilities, providing unprecedented levels of situational awareness and operational flexibility. As technology evolves, continued research and development are essential to address challenges, maximize benefits and ensure the responsible use of AI in Naval operations.

#### 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; Task 1.2.1. Research and application of land, water and unmanned aerial vehicles for logistics, acquisition and remote transmission of sensor and visual information

#### REFERENCES

[1] B. Auslander, K. Gupta and D. Aha, "Maritime Threat Detection using Plan Recognition," in Proc. IEEE Conference on Technologies for Homeland Security (HST) 2012, Available:

<https://apps.dtic.mil/sti/tr/pdf/ADA570824.pdf> [Accessed February 14, 2024], DOI: 10.1109/THS.2012.6459857

[2] Zh. Yordanov, "Monitoring systems of national sea spaces. Interaction and information exchange," in Proc. International scientific conference "MIA 2030", Burgas, Bulgaria, 2022, p.131-139

[3] J. Dittmer, "The state, all at sea: Interoperability and the Global Network of Navies", Sage Journals, vol. 39, no. 7, pp. 1389-1406, 2021. Available: <https://journals.sagepub.com/doi/abs/10.1177/2399654418812469>. [Accessed February 15, 2024]. DOI: <https://doi.org/10.1177/2399654418812469>

[4] K. Steen-Tveit and B. Munkvold, "From common operational picture to common situational understanding: An analysis based on practitioner perspectives," Journal Safety Science, Vol. 142, October 2021. [Online]. Available: Sciencedirect, <https://www.sciencedirect.com/science/article/pii/S0925753521002253>. [Accessed February 15, 2024]. DOI: <https://doi.org/10.1016/j.ssci.2021.105381>

[5] D. Markov, "Challenges to International relations and international security in the age of Artificial intelligence," in Proc. of an Annual University Scientific Conf., V. Levski National University, Veliko Tarnovo, Bulgaria, 2021, pp. 296-304

[6] V. Vassilev, "The changing importance of the National maritime spaces and the implications for maritime security," in Proc. International Scientific Conference "105 years of knowledge in the interest of security and defense" Vol.1, Rakovski NDC, Sofia, Bulgaria, 2018, pp. 146-150

[7] B. Johnson, "Challenges in Implementing Artificial Intelligence for Naval Warfare", Naval Engineers Journal, vol. 135, no. 1, pp. 95-103(9), March 1, 2023. Available: <https://www.ingentaconnect.com/contentone/asne/nej/2023/00000135/00000001/art00020>. [Accessed February 18, 2024].

[8] B. Johnson and W. Treadway, "Artificial Intelligence – An Enabler of Naval Tactical Decision Superiority", AI Magazine, vol. 40, no. 1, pp. 63-78, Spring 2019. Available: <https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/2852>. [Accessed February 17, 2024]. DOI: <https://doi.org/10.1609/aimag.v40i1.2852>

[9] I. B. Tsekov, "Cyber sovereignty as a new form of state presence on the Internet," Journal "Savremennopravo", Vol.1, pp.15-24, 2020

[10] S. M. Hogge, "Robotic and Artificial Intelligence Systems for the Naval Operational Environment", Naval Engineers Journal, vol. 99, no. 4, pp. 74-86(13), July 1, 1987. Available: <https://www.ingentaconnect.com/content/asne/nej/1987/00000099/00000004/art00017>. [Accessed February 18, 2024]. DOI: <https://doi.org/10.1111/j.1559-3584.1987.tb02159.x>

[11] A. Munir, A. Aved and E. Blasch, "Situational Awareness: Techniques, Challenges, and Prospects," AI, vol. 3(1), pp. 55-77, Jan 2022. Available: <https://www.mdpi.com/2673-2688/3/1/5> [Accessed January 25, 2024], <https://doi.org/10.3390/ai3010005>

[12] R. Marinov, "Perspectives of Intelligent Technologies Based on Artificial Intelligence," in Proc. Scientific conference "110 Years of Knowledge", Rakovski NDC, Sofia, Bulgaria, 2022, pp. 91-98

# *Analytical model for determining the friction force at the contact of a metal body with a copper contact surface*

**Yana Dimitrova**

Department of Armaments and design technology  
National Military University "Vasil Levski"  
Shumen, Bulgaria  
[yaddimitrova@nvu.bg](mailto:yaddimitrova@nvu.bg)

**Abstract.** The paper presents the development of an analytical model for calculating the frictional force when a copper contact surface slides across a static metallic body. Available analytical tribological models and mathematical methods were used to create the model. This model can be used to obtain information about the barrel wear of an artillery gun.

**Keywords:** Analytical model, sliding motion, friction force, tribology.

## I. INTRODUCTION

The motions of elements relative to each other is related to the occurrence of frictional forces. These frictional forces are an undesirable phenomenon in most machine elements, as they lead to material wear.

The tribology science deals with the study of frictional forces, the lubrication, the performance and reliability of machine elements. It is the basis for developing and implementing methods to increase the wear resistance of machine elements.

These methods are based on derived mathematical dependencies and analytical models to determine and research frictional forces. In the available literature on tribology, a wide variety of derived and proven dependencies and models for determining the values of friction forces at various contact interactions of machine elements are observed [2], [3], [6], [10], [11], [13], [16], [17], [18], [20], [22].

This dependence mainly affects general purpose machine elements. Models for determining the frictional forces of special-purpose machine elements are more difficult to reach. As a result, it is necessary to carry out a study of the contact characteristics of the researched special purpose machine elements and the available dependencies and models. In this way, it is possible to

develop a useful analytical model for studying the research problem.

The artillery tube is one such a special purpose machine element. In the artillery tube, a frictional force occurs as a result of the motion of the projectile in their bore. The contact interaction is between the chrome-nickel coating of the inner surface of the artillery tube and the copper rotating band of the projectile [12].

The report presents an analytical model for evaluating and determine the frictional force that occurs in contact between artillery tube and projectile rotating band. The dependencies and models used are for the determination of friction forces and their calculation in the development of various machine elements and details.

## II. MATERIALS AND METHODS

In recent years, the dependences for determining the parameters of certain tribological variables have been increasing more and more. The wide variety of existing dependencies for calculating and determining frictional forces makes it almost impossible to cover them completely. Therefore, the report covers the main, most accessible and most frequently used dependencies for determining the tribological processes occurring at the contact of two elements, related to the studied problem.

Excluding the specific conditions of the studied problem and considering the motion of the projectile through the bore of artillery tube, as a contact scheme, it can be concluded that the following forces occurs in this process:

- sliding friction force;
- rotating friction force;
- frictional force from the flow of the gunpowder gases;

Print ISSN 1691-5402  
Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8197>

© 2024 Yana Dimitrova. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).



- adhesion friction force.

For develop the model, analytical dependencies are used, which approach the contact scheme of the problem under research. These dependencies have been redone using general mathematical principles to more fully represent the researched frictional force.

In developing the model is used the same one characteristic, which corresponds to the same one variable. Accordingly, once written, the variable will not be written further in the paper.

Based on the analysis made of the available literature [2], [4], [5], [8], [9], [12], [19], [21], it is assumed that for the projectile-artillery tube contact scheme, hydrodynamic friction forces must be taken into account since there is presence of gunpowder gases moving between the two elements [2], [3], [6], [10], [13], [17], [18], [20]. Consideration of these hydrodynamic friction forces is imperative due to the fact that the presence of even a minimal amount of fluid significantly changes the nature of the friction forces.

Accordingly, in the determination of the dynamic force of sliding friction (occurring during the forward motion of the projectile), the widely accepted Newtonian relation for hydrodynamic friction can be used [18], [20]:

$$F_{sl} = \eta \cdot S_a \cdot G \quad [\text{N}] \quad (1)$$

where:  $F_{sl}$  – sliding friction force [N];  
 $\eta$  – dynamic viscosity of the fluid [Pa.s];  
 $S_a$  – nominal contact area [m<sup>2</sup>];  
 $G$  – velocity gradient [s<sup>-1</sup>].

Velocity gradient it can be determined by [18], [20]:

$$G = \frac{v}{h_d} \quad [\text{s}^{-1}] \quad (2)$$

where:  $v$  – velocity of the linearly moving element [m/s];  
 $h_d$  – clearance between the two elements in contact [m].

In addition, as a result of the viscosity of the fluid present in the contact between the two elements and their very rapid separation, the viscous friction force (friction force caused by the flow of the gunpowder gases) occurs. The dependency derived to calculate this force is [3]:

$$F_v = \frac{h_d^2 \cdot \eta}{t_s} \quad [\text{N}] \quad (3)$$

where:  $F_v$  – viscous friction force [N];  
 $t_s$  – the required time to separate the two contact elements [s].

The analysis of the wear mechanism of the artillery tube shows that during the movement of the projectile in the bore of the gun tube, a frictional adhesion force also occurs. This friction force occurs as a result of the high-speed progressive and rotational motion of the projectile accompanied by high temperature and pressure of the burning gunpowder composition. In this process, the metal composition of the artillery tube coating and the

rotating band of the projectile is liquefied, which can lead to adhering of surface asperity. In addition, the small clearance between the projectile and the artillery tube bore creates compression of their surface layers under the action of normal loading.

In the conditions of liquid-mediated contact, the determination of adhesion friction force can be done using the model of McFarlane and Tabor [3]:

$$F_a = \frac{\partial^2 \cdot \eta}{t_s} \quad [\text{N}] \quad (4)$$

where:  $F_a$  – adhesion friction force [N];  
 $\partial$  – proportionality constant (dimension of length) [m<sup>2</sup>].

The models described so far present information only about the individual frictional forces that occur in the contact of the projectile with the artillery tube.

In order to more accurately determine the friction forces occurring when two elements are in contact and to obtain more reliable data, it is necessary to collect the individual friction forces.

Thus, for example, if it is assumed that there is a negligible interaction between adhesion and deformation processes during sliding (dynamic friction force), they can be collected [18], [20] to obtain the total friction force, or:

$$F_p = F_a + F_d \quad [\text{N}] \quad (5)$$

where:  $F_p$  – total friction force [N];  
 $F_d$  – dynamic friction force [N].

In another part of the studied available literature sources, even with the slightest presence of any fluid, the following dependence is presented for determining the total friction force [3]:

$$F_p = \mu_p \cdot (W + F_d) + F_v \quad [\text{N}] \quad (6)$$

where:  $\mu_p$  – coefficient of friction;  
 $W$  – normal load [N].

As a disadvantage of this dependencies, it can be pointed out that they do not take into account all the frictional forces occurring in the contact scheme of the problem under research.

For the precise calculation and determination of the coefficient of friction, various dependencies have been derived that apply to specific contact elements under certain operating conditions. Thus, for example, with an adhesive friction force present at plastic deformation, the coefficient of friction can be determined by means of the equation [3]:

$$\mu_s = \frac{\tau_a}{H} \quad (7)$$

where:  $\mu_s$  – coefficient of friction at condition of adhesion and plastic deformation;  
 $\tau_a$  – shear stress [N/m<sup>2</sup>];  
 $H$  – hardness of softer element [N/m<sup>2</sup>].

To determine the shear stress, according to the Hertzian model, for a circular contact surface, the equation is used [3]:

$$\tau_a = 0.31 \cdot p_o \quad [\text{N/m}^2] \quad (8)$$

where:  $p_o$  – maximum contact pressure  $[\text{N/m}^2]$ .

The maximum contact pressure can be determined using the equation [3]:

$$p_o = \left( \frac{6 \cdot W \cdot E^* \cdot \pi^2}{\pi^3 \cdot \mathcal{R}^2} \right)^{\frac{1}{3}} \quad [\text{N/m}^2] \quad (9)$$

where:  $E^*$  – composite modulus of elasticity  $[\text{N/m}^2]$ ;  
 $\pi = 3,14$  – Archimedes' Constant;  
 $\mathcal{R}$  – composite radius  $[\text{m}]$ .

The normal load –  $W$  is determined using the equation [3]:

$$W = \frac{4 \cdot N \cdot E^* \cdot S_w^{\frac{3}{2}}}{3 \cdot \pi^2 \cdot \mathcal{R}} \quad [\text{N}] \quad (10)$$

where:  $N$  – number of asperities on the roughness;  
 $S_w$  – real contact area  $[\text{m}^2]$ .

The following equation is used to determine the composite radius [3], [6]:

$$\frac{1}{\mathcal{R}} = \frac{1}{R_1} + \frac{1}{R_2} \quad [\text{m}] \quad (11)$$

where:  $R_1$  – principal radii of curvature for the first element in the contact scheme  $[\text{m}]$ ;  
 $R_2$  – principal radii of curvature for the second element in the contact scheme  $[\text{m}]$ .

To determine the composite modulus of elasticity, the following equation is given [3], [6], [18]:

$$E^* = \frac{1-v_1^2}{E_1} + \frac{1-v_2^2}{E_2} \quad [\text{N/m}^2] \quad (12)$$

where:  $E_1$  – Young's modulus of elasticity for the first element in the contact scheme  $[\text{N/m}^2]$ ;  
 $E_2$  – Young's modulus of elasticity for the second element in the contact scheme  $[\text{N/m}^2]$ ;  
 $v_1$  – Poisson's ratio for the first element in the contact scheme;  
 $v_2$  – Poisson's ratio for the second element in the contact scheme.

When determining the real contact area, in case of plastic deformations, the following equation can be used [3], [18]:

$$S_w = \frac{W}{H} \quad [\text{m}^2] \quad (13)$$

Some of the dependencies reviewed so far have been analysed and presented in a source [23].

### III. RESULTS AND DISCUSSION

In accordance with what has been reviewed so far and the analysis presented in [23], in the equation – 5 and 6 it is necessary to replace the dynamic frictional force with the frictional force caused by the sliding motion of the projectile in the gun tube bore. As a result, using equation 5 and 6 and collecting the individual frictional forces that occur in contact between the projectile and the inner surface of the artillery tube bore to determine the total frictional force is obtained:

$$F = \mu \cdot (W + F_{sl}) + F_v + F_a \quad [\text{N}] \quad (14)$$

From the solution of the equation 11, to determine the compound radius is obtained:

$$\mathcal{R} = \frac{R_s \cdot R_k}{R_s + R_k} \quad [\text{m}] \quad (15)$$

where:  $R_s$  – projectile radius  $[\text{m}]$ ;  
 $R_k$  – artillery tube bore radius  $[\text{m}]$ ;

Substituting equations 10 and 15 into equation 13, to determine the real contact area is obtained:

$$S_w = \frac{4 \cdot N \cdot E^* \cdot S_w^{\frac{3}{2}}}{3 \cdot \pi^2 \cdot \mathcal{R} \cdot H} \quad [\text{m}] \quad (16)$$

After substituting equations 12 and 15 into equation 16 and solving the resulting equation, to determine the real contact area is obtained:

$$S_w = \frac{9 \cdot \pi^3 \cdot \left( \frac{R_s \cdot R_k}{R_s + R_k} \right)^2}{16 \cdot N^2 \cdot E^{*2} \cdot H^2} \quad [\text{m}] \quad (17)$$

By substituting equations 12, 15 and 17 into equation 10 to determine, the normal load the following dependency is obtained:

$$W = \frac{4 \cdot N \cdot \left( \frac{1-v_1^2}{E_1} + \frac{1-v_2^2}{E_2} \right) \cdot 9 \cdot \pi^3 \cdot \left( \frac{R_s \cdot R_k}{R_s + R_k} \right)^2}{3 \cdot \pi^2 \cdot \frac{R_s \cdot R_k}{R_s + R_k}} \quad [\text{N}] \quad (18)$$

After performing a mathematical conversion, to determine the normal load is obtained:

$$W = \frac{3 \cdot \pi^{\frac{3}{2}} \cdot R_k \cdot R_s}{4 \cdot N \cdot H^2 \cdot (R_s + R_k)} \quad [\text{N}] \quad (19)$$

To determine the sliding friction force, it is necessary to determine the nominal contact area. In accordance with this, the general principles of mathematics and the fact that the projectile has a complex shape, the nominal contact area should be divided into two parts - a conical part and a cylindrical part. Then, to determine the nominal contact area is obtained [7]:

$$S_a = (2 \cdot \pi \cdot r_{cy} \cdot l_{cy}) + (\pi \cdot r_{co} \cdot c) \quad [\text{m}^2] \quad (20)$$

where:  $r_{cy}$  – radius of the cylindrical part of the projectile [m];  
 $l_{cy}$  – height of the projectile cylindrical part [m];  
 $r_{co}$  – radius of the base of the projectile cone [m];  
 $c$  – slant height of the projectile cone [m].

To determine the slant height of the projectile cone, the following equation is given [7]:

$$c = \sqrt{r_{co}^2 + l_{co}^2} \quad [\text{m}] \quad (21)$$

where:  $l_{co}$  – height of the projectile cone [m].

Substituting equation 21 into equation 20, for determining the nominal contact area is obtained:

$$S_a = (2 \cdot \pi \cdot r_{cy} \cdot l_{cy}) + (\pi \cdot r_{co} \cdot \sqrt{r_{co}^2 + l_{co}^2}) \quad [\text{m}^2] \quad (22)$$

It is necessary to select equation for determining the clearance between the projectile and the artillery tube bore. According to the deformation theory, it can be used [14]:

$$h = S_s - S_k = \pi \cdot (R_s^2 - R_k^2) \quad [\text{m}^2] \quad (23)$$

where:  $S_s = \pi R_s^2$  – projectile area [m<sup>2</sup>];  
 $S_k = \pi R_k^2$  – the gun tube bore area [m<sup>2</sup>];

By substituting equations 2, 22 and 23 into equation 1 to determine, the sliding friction force following dependency is obtained:

$$F_{sl} = \frac{\eta \cdot \left[ (2 \cdot \pi \cdot r_{cy} \cdot l_{cy}) + (\pi \cdot r_{co} \cdot \sqrt{r_{co}^2 + l_{co}^2}) \right] \cdot V_d}{\pi \cdot (R_s^2 - R_k^2)} \quad [\text{N}] \quad (24)$$

where:  $V_d$  – projectile forward velocity [m/s];

To determine viscous friction force, it is seen from equation 3 that it is necessary to determine the time required for the projectile to pass through artillery tube. This can be obtained through [1], [15]:

$$t_1 = \frac{l_0}{V_d} \quad [\text{s}] \quad (25)$$

where:  $t_1$  – time required for the projectile to pass through artillery tube [s];

$l_0$  – length of the rifled part of the artillery tube [m];

Substituting equations 23 and 25 into equation 3, to determine the viscous friction force is obtained:

$$F_v = \frac{[\pi \cdot (R_s^2 - R_k^2)]^2 \cdot \eta}{\frac{l_0}{V_d}} = \frac{[\pi \cdot (R_s^2 - R_k^2)]^2 \cdot \eta \cdot V_d}{l_0} \quad [\text{N}] \quad (26)$$

Substituting equation 25 into equation 4, to determine the adhesion friction force is obtained:

$$F_a = \frac{\partial^2 \cdot \eta \cdot V_d}{l_0} \quad [\text{N}] \quad (27)$$

Substituting equations 12, 15 and 19 into equation 9, and performing a mathematical conversion, to determine the maximum contact pressure is obtained:

$$p_0 = \left[ \frac{(9 \cdot R_s + 9 \cdot R_k) \cdot (E_2 - v_1^2 \cdot E_2 + E_1 - E_1 \cdot v_2^2)^2}{2 \cdot \pi^2 \cdot E_1 \cdot H^2 \cdot R_k \cdot N \cdot R_s \cdot E_2^2} \right]^{\frac{1}{3}} \quad [\text{N/m}^2] \quad (28)$$

After substituting equation 28 into equation 8, to determine the shear stress is obtained:

$$\tau_a = 0.31 \cdot \left[ \frac{(9 \cdot R_s + 9 \cdot R_k) \cdot (E_2 - v_1^2 \cdot E_2 + E_1 - E_1 \cdot v_2^2)^2}{2 \cdot \pi^2 \cdot E_1 \cdot H^2 \cdot R_k \cdot N \cdot R_s \cdot E_2^2} \right]^{\frac{1}{3}} \quad [\text{N/m}^2] \quad (29)$$

After substituting equation 29 into equation 7, for determining the coefficient of friction, is obtained:

$$\mu_s = \frac{0.31 \cdot \left[ \frac{(9 \cdot R_s + 9 \cdot R_k) \cdot (E_2 - v_1^2 \cdot E_2 + E_1 - E_1 \cdot v_2^2)^2}{2 \cdot \pi^2 \cdot E_1 \cdot H^2 \cdot R_k \cdot N \cdot R_s \cdot E_2^2} \right]^{\frac{1}{3}}}{H} \quad (30)$$

Substituting equations 19, 24, 26, 27 and 30 into equation 14, the analytical model for determining the friction force at the contact of a metal body with a copper contact surface is derived:

$$F = \frac{0.31 \cdot \left[ \frac{(9 \cdot R_s + 9 \cdot R_k) \cdot (E_2 - v_1^2 \cdot E_2 + E_1 - E_1 \cdot v_2^2)^2}{2 \cdot \pi^2 \cdot E_1 \cdot H^2 \cdot R_k \cdot N \cdot R_s \cdot E_2^2} \right]^{\frac{1}{3}}}{H} \cdot \left[ \frac{3 \cdot \pi^2 \cdot R_k \cdot R_s}{4 \cdot N \cdot H^2 \cdot (R_s + R_k)} + \frac{\eta \cdot \left[ (2 \cdot \pi \cdot r_{cy} \cdot l_{cy}) + (\pi \cdot r_{co} \cdot \sqrt{r_{co}^2 + l_{co}^2}) \right] \cdot V_d}{\pi \cdot (R_s^2 - R_k^2)} \right] + \frac{[\pi \cdot (R_s^2 - R_k^2)]^2 \cdot \eta \cdot V_d}{l_0} + \frac{\partial^2 \cdot \eta \cdot V_d}{l_0} \quad [\text{N}] \quad (31)$$

#### IV. CONCLUSIONS

Through the derived model, it is possible to theoretically determine the friction force that occurs when a metal body contacts a copper contact surface, such as the inner surface of an artillery tube bore and the rotating band of a projectile.

The model derivation is a step in the process of developing an algorithm for determining artillery tube bore wear. Such an algorithm is necessary for theoretical research and studying related to the construction of artillery tube.

The development of an algorithm for determining the wear resistance of artillery tube requires a more in-depth analysis of the processes leading to the artillery tube wear. This algorithm should include sequentially coupled analytical models to determine and study the wear processes of the artillery tube.

Through this algorithm it can be possible to perform theoretical research. Research is an important stage of scientific work, as through them data can be collected from the obtained results.

As a result, by comparing the results with those obtained from empirical research and using statistical methods, the adequacy of the developed analytical model can be assessed.

#### ACKNOWLEDGMENTS

The report is being carried out under the National Scientific Program "Security and Defense," adopted by Council of Ministers Decree № 731 of October 21, 2021, and in accordance with Agreement № D01-74/19.05.2022.



#### REFERENCES

- [1] A. Lahiri, Basic physics: Principles and concepts. Fourth revision. I., 2017.
- [2] A. Tuktanov, Production process of small arms gunnery and artillery weapons. M., 2007.
- [3] B. Bhushan, Introduction to Tribology. 2nd Edition. USA, 2013.
- [4] B. J. Heard, Handbook of firearms and ballistics: Examining and interpreting forensic evidence. Second edition. John Wiley & Sons, 2008.
- [5] D. E. Carlucci and Jacobson S. S., Ballistics: Theory and design of guns and ammunitions. N.Y.: CRC, 2007.
- [6] H. Rebai, „Tribology and machine elements: Mechanical engineering and production technology,“ B. thesis, University of applied sciences. Riihimäki: HAMK, 15.08.2014.
- [7] J. Bennett and W. Briggs, Using and understanding mathematics: A quantitative reasoning approach. Seventh edition. Boston: Pearson, 2019.
- [8] J. Jain, S. L. Soni and D. Sharma, “Determination of wear rate equation and estimation of residual life of 155 mm autofrettaged gun barrel,” Int. Jnl. of Multiphysics, Volume 5, Number 2011. Available: Research Gate <https://www.researchgate.net/>. [Accessed February 5, 2024].
- [9] J.-s. Ma, „The law of barrel wear and its application,“ Defence Technology, Volume 14, Issue 6, pp. 674-676, December 2018. [Online]. Available: Scince Direct, <https://www.sciencedirect.com>. [Accessed February 3, 2024].
- [10] M. J. Neale, The tribology handbook. Second edition. BH, 2001 г.
- [11] R. C. Juvinall and K. M. Marshek, Fundamentals of machine component design. Fifth Edition. Wiley, 2012.
- [12] R. G. Hasenbein, “Wear and erosion in large caliber gun barrels,“ Defence technical information centre, 2004, [Online]. Available: DTIC, <https://apps.dtic.mil/>. [Accessed February 9, 2024].
- [13] V. Yastrebov, G. Anciaux and Eds., From infinitesimal to full contact between rough surfaces: Evolution of the contact area. HAL, 13.08.2015 г.
- [14] А. Дж. Зукас, Т. Николас и Х. Ф. Свифт, Динамика удара. М.: Мир, 1985.
- [15] А. Ю. Григорьев, Д. П. Малякко и Л. А. Федорова Теоретическая механика: Кинематика. Учеб. пособие. СПб.: НИУ ИТМО; ИХиБТ, 2013.
- [16] Б. П. Сафонов и А. В. Бегова, Инженерная трибология: Оценка износостойкости и ресурса трибосопрежений. Новомосковск, 2004.
- [17] В. Л. Попов, Механика контактного взаимодействия и физика трения: От нанотрибологии до динамики землетрясений. Москва: Физматлит, 2013
- [18] И. И. Беркович и Д. Г. Громаковский, Трибология: Физические основы, механика и технические приложения. Самара, 2000.
- [19] К. Г. Калев, Влияние на изменението на геометрията на канала върху баллистичните параметри на оръдейното тяло. Шумен, 2017.
- [20] М. Кандева, Инженерна трибология: Цикъл лекции за докторанти, ТУ-София: МТФ, 2012.
- [21] М. Серебреков, Вътрешна балистика. София, 1996.
- [22] Н. Манолов и М. Кандева, Обща трибология. София, 2004.
- [23] Я. Димитрова, „Анализ на аналитичните модели за определяне силите на триене възникващи при контакта на въртеливо и постъпателно движещо се метално тяло с полимерен материал“, Сборник доклади от научна конференция „Логистиката и обществените системи“, електронно издание, Издателски комплекс НВУ „В.Левски“, 2021, с. 252-261, ISSN 2738-8042

# Evaluation of wear mechanism of special purpose machine elements

Yana Dimitrova

Armaments and design technology department  
National Military University Vasil Levski  
Shumen, Bulgaria  
[yaddimitrova@nvu.bg](mailto:yaddimitrova@nvu.bg)

**Abstract.** The purpose of the paper is to evaluate the wear mechanism that occur in the artillery armament main part – gun tube. In order to achieve this purpose, the mechanism of wear has been derived by means of studying the information from literary sources and drawing conclusions. The topicality of the topic is dictated by the constant aspiration of scientists to derive a new theory, reduce the manufacturing resources and increase the wear resistance of the gun tube. The study of the problem led to an assessment of the processes occurring in the gun tube of the artillery system. As a result of the study, it can be pointed that a different theory of the wear mechanism of special purpose machine elements has been established.

**Keywords:** Machine elements, tribology, wear.

## I. INTRODUCTION

The classification - special-purpose machine elements of a gun tube of an artillery system is derived from that they are thick-walled tube with unique purpose. Their purpose is to give direction and certain values of progressive and rotating motion of the projectile.

Approximately 85% of their inner surface is cut in the shape of a groove that curve from left to right and up. These grooves are designed to coerce the projectile to rotate about its longitudinal axis. This, in turn, gives the projectile stability during its flight.

The rest of the inner surface is made smoothbore in the shape of the cartridge case of the ammunition intended for it. This part is located at the rear end of the tube.

Behind the rear end of the tube, it is located a special detail that closes it when a shot is fired.

To produce a shot, it is necessary to place the projectile and the cartridge case in the tube. This process is called loading. During the loading process projectile rotating band its cut into the grooves of the tube. The rotating band it represents a copper or copper-nickel ring made on the cylindrical part of the projectile. The purpose of the rotating band is to give the projectile revolutions of rotation around the longitudinal axis and to obturate the gunpowder gases during the shot.

As a result of the projectile loading and closing the rear end of the tube, a chamber is obtained. In this chamber, during the shots fire production, the gunpowder burns. As a result of this process, a force is formed that produces the initial forward and angular velocity of the projectile.

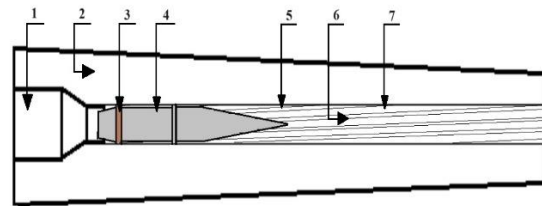


Fig. 1. Schematic diagram of an artillery gun barrel

1 – chamber; 2 – gun tube; 3 – rotating band; 4 – projectile;  
5 – land; 6 – bore; 7 – groove.

The combustion of gunpowder, along with the projectile movement in the bore of the tube, causes wear on the gun tube. The wear, in turn, leads to decrease in the combat effectiveness of the artillery systems.

The problem exploration and finding ways to extend the wear resistance of gun tube it's an important scientific task. This task is derived from the striving to extend the resource of gun tube shots and increase the combat effectiveness of the artillery systems.

What has been written so far is based on general conclusions drawn from the study of the information from the sources [1], [3], [4], [10] and [20].

It is written in [6] that gun tube wear is a complex phenomenon and no single wear prediction theory is suitable for tube wear. It is shown in [6] and [7] that many scientists have established different theories, but there are still other scientists who try to approach in a different way to understand and increase the wear resistance of the gun tube, for example [7], [10], [15] and [17].

Print ISSN 1691-5402  
Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8198>

© 2024 Yana Dimitrova. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

This, together with the fact that theoretical research reduces the manufacturing resource, gives the topicality of the topic of the paper.

In addition, the purpose of the paper is to establish the mechanism of wear of the special purpose machine elements. To achieve this purpose, the wear mechanism is described based on summarized information from the described references at the end of the paper.

## II. MATERIALS AND METHODS

The gun tube is made of alloy steel, with a coating applied to their inner surface. This coating aims to satisfy and increase the tactical and technical requirements of the gun tube. To these requirements refer: hardness, wear resistance, corrosion resistance, damage resistant, heat resistance, etc. [15].

However, as a result of the shot phenomenon, the gun tube is under the influence to severe intense thermodynamic and tribological wear. Wear character is not unique, it depends on the Caliber of the system and the number of shots fired per minute [6], [7].

Wear can be defined as loss of material, destruction of the metal net of the materials and change in the geometric characteristics of the elements. It is obtained as a result of the contact interaction between the elements during the movement of even just one of them. During sliding, rolling and even impact motion of one detail relative to another, the asperity of the interacting materials change the properties of the surfaces. This leads to the appearance of surface wear, which gradually increases to material loss.

Wear is influenced by the physio-chemical properties of the materials, as well as those of the contact environment. It is a complex process that is difficult to describe with the influence of single factor. For this reason, there are different types of wear that depend on the character of the contact surfaces and the properties of the surrounding environment of the contacting elements.

Based on this, it is necessary to clarify the processes occurring in the gun tube and to evaluate the mechanisms leading to its wear.

Researching the processes occurring in a gun tube, they can be divided into:

- loading the projectile in the bore of the gun tube;
- ignition of the gunpowder;
- formation of temperature and pressure from the burning gunpowder;
- formation a force causing the sliding motion of the projectile;
- rotating of projectile in the bore of the gun tube.

In the first process, impact wear occurs. This wear is characterized by two phenomena: erosion or percussion.

Erosion occurs as a result of the kinetic energy of solid particles present in the surrounding environment or liquid droplets of steam and their subsequent aggressive action on the material [2], [5]. Erosion wear occurs as a result of the flow generated by the high velocity of the burning gunpowder composition.

Erosion also occurs as a result of the fact that the process of loading the system takes place in environments

with different concentrations of dust particles. As a result, there are various abrasive particles adhering to the rotating band. These abrasive particles contribute to increase the wear. In such cases, wear is called erosive-abrasive [18].

Percussion is developed by continuously repeating impact action on a metal detail. In the gun tube bore, percussion phenomena can be explained by the fact that during loading process the projectile is pushed into the bore with certain force. This process results in the projectile impacting the bore of the gun tube.

During the process of combustion gunpowder, temperature and pressure are form, which quickly increase to large values. This coerces the metal to expand. As the temperature and pressure drop, the metal returns to its original dimensions. Constant expansion and constriction lead to fatigue of the metal structure, which over time turns into a net of microcracks. Gradually, pieces of the metal break off from these microcracks.

The high temperature generated by the combustion of the gunpowder composition causes the metal to melt. This, in turn, contributes the wear mechanism to occur more intensive, as the molten metal deforms more easily.

In addition, the products of gunpowder combustion lead the chemical erosion of the metal [17]. A chemical reaction occurs during this process. This reaction can be explained by the interaction of the chemical products of the gunpowder composition with the surface layer of the metal. As a result of this reaction, the undesirable phenomena - corrosion and oxidation - are formed.

In cases where there is no motion of the elements, the chemical products of oxides can form a chemical film to protect the metal from corrosion. But the sliding motion of the detail wears away the chemical film and so the chemical reaction continues to develop. From this it can be concluded that chemical erosion requires both a chemical reaction and friction caused by motion of the workpiece [2].

Chemical wear gradually leads to the destruction of the surface layer of the material. Parts operating in a corrosive environment wear out faster than those that are not in such an environment.

But the gunpowder combustion also resulting to formation of pressure. This pressure forms the force that causes the projectile sliding motion. In the result, projectile acquires a forward velocity which gradually increases and reaches maximum value when the projectile exits the muzzle cut. As the projectile slides, it also begins to rotate.

In these motions occurs *adhesion wear*, *abrasive wear* and *fatigue wear*.

What has been written so far and what is yet to be written next is based on summary conclusions from a study of the information from the sources [2], [5], [8], [9], [12], [13], [14], [16], [17], [19] and [21].

During the movement of one body relative to another, the contact between them is formed at the tips of their asperity. The asperities are located on to the surface layers.

The characteristics of the surface layers are relevant to the interaction because they affect the actual area of contact, friction, and wear [2], [11]. The surface layers of the elements consist of micro and macro asperities (Fig. 2. – line „2” and „3”), which depends on the accuracy and method of manufacturing the machine elements.

In the movement of one element relative to another, the friction force is due to the contact of the asperity of the materials, where contact region is formed (Fig. 2. – „b”).

The contact region, in turn, forms the contact area (Fig. 2. – „b”), which consists of asperity of different heights (Fig. 2. – line „1”).

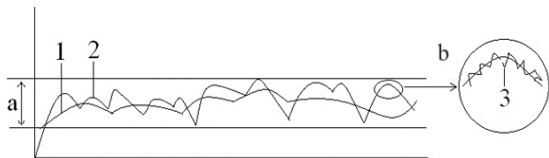


Fig. 2. An image of the asperity of the surface layers.

a – real contact surface; b – contact region;  
1 – asperity; 2 – macro asperity; 3 – micro asperity.

The high stress on the tips of the asperity in the contact regions, when two elements are pressed against each other either under the action of the normal loading or under the action of combined normal or shear stresses, causes them to stick together, forming so-called contact bridges. As a result, in order to separate these contact bridges, a frictional force, called the adhesion frictional force, occur on the surfaces during relative sliding motion [2], [5].

The frictional adhesion force causes *adhesive wear*, which occurs as a result of the rupture of the contact bridges. This process concludes with tearing off a fragment from one surface and adhering it to the other surface. With continued sliding, this fragment can be attached to the original surface or completely removed. This process is influenced by the physical and chemical properties of the contacting elements and the environment in which they interact.

*Abrasive wear* occurs when elements in contact have a significant difference in hardness. In abrasive wear, the asperity of the harder material penetrates the surface of the softer material and fracture it. This fracture, with continued motion of the elements, develops into removal of material, in the form of thin chips or a whole fragment, from the surface of the softer element. In addition, this process is associated with damage to the surface through plastic deformation. In abrasive wear, the deformation of metals associated with it is considered in three ways: cutting, plowing and wedge formation [2].

Abrasive wear also occurs when there are solid particles between contacting elements. This makes abrasive wear similar to erosive wear. The difference

between these two types of wear is that in erosive wear, the solid particles must have their own driving force.

In the bore of the gun tube under the action of the burning gunpowder, the subsequent sliding and rotating motion of the projectile, the solid particles that have caught move around the rotating band and the bore. They have their own driving force, but during loading of the projectile into the gun tube, these solid particles will fracture the bore on the inside of the gun tube.

As a result of the above, it can be assumed that abrasive and erosive wear are processes that bring the gun tube to wear.

The constantly repeated loading and firing processes lead to *fatigue wear*. Fatigue wear of the material usually occurs after repeated cycles of sliding, rolling and impact, even with negligible friction. These cycles are associated with loading and unloading of the wear detail. Under loading process, the performing action of the wearing detail is taken into account. For the gun tube, the loading and firing processes represent this action.

These cycles can lead to surface and subsurface cracks. Gradually, these cracks develop into the breakdown of material and pits formation.

The sliding and rotating motion of the projectile in the bore of the gun tube are assumed to be complex motions. As a result of these motions, frictional stresses arise, which cause shearing stresses in the contact region. In this way, a cyclic deformation is formed in the surface layer, which gradually develops into surface fatigue.

The sliding motion is usually higher, comparable to rolling motion observed in a process of wear. During the sliding motion, the adhesion and abrasion processes develop through the asperity of the surface layers of the contacting elements. In these processes it is possible the asperity to pass each other without adhering or abrading, but this causes them undergo to plastic deformation. In continuous cycles of this deformation cracks form and extend due to fatigue of the material, which gradually results to the loss of fragments of the metal.

Through new technologies, it is possible to simulate and study the described processes in a virtual environment.

New technologies provide an ability to construct virtual prototypes of an existing or future product to be studied through the specialized software products for engineering analysis. This would help to create new series of products with changed characteristics [11].

### III. RESULTS AND DISCUSSION

As a result of the described processes, the wear mechanisms of special purpose machine elements, which is the gun tube of an artillery system, can be summarized.

Print ISSN 1691-5402  
Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8198>

© 2024 Yana Dimitrova. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).



Figure 3 shows the approximate sequence of processes leading to wear of the gun tube of artillery systems. This can be a starting point for more in-depth research of the problem related to the wear of artillery tube.

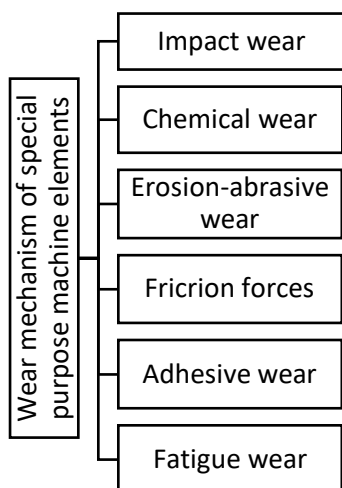


Fig. 3. Approximate consecution of wear mechanism of special purpose machine elements

The derivation of the mechanism of wear of artillery tube is based on a research of available literature sources relating to the wear of machine elements. Specialized literature related to the processes occurring in the artillery tube during its firing was also used.

To clarify the credibility of the derived mechanism, it is necessary to establish a methodology for studying the wear of the bore of the gun tube.

Establishing of such a methodology requires the consistent development of analytical models taking into account the frictional forces and the resulting amount of wear.

The represented wear mechanism can assist the process of deriving the analytical models of wear. The development of the models is necessary to perform theoretical researches and to have the opportunity to predict the number of shots before the final failure of the gun tube occurs.

#### IV. CONCLUSIONS

Through research and drawing conclusions on the basis of literary information on the studied problem, a wear mechanism of special purpose machine elements has been established.

This mechanism is necessary to develop a methodology for predicting the wear resistance of the gun tube. The ability to predict the gun tube wear resistance is an important part of scientific work for the education and advancement of the engineer involved in the design of artillery systems.

#### ACKNOWLEDGMENTS

The report is being carried out under the National Scientific Program "Security and Defense," adopted by Council of Ministers Decree № 731 of October 21, 2021, and in accordance with Agreement № D01-74/19.05.2022.

#### REFERENCES

- [1] A. Tuktanov, Production process of small arms gunnery and artillery weapons. M., 2007.
- [2] B. Bhushan, Introduction to Tribology. 2nd Edition. USA, 2013.
- [3] B. J. Heard, Handbook of firearms and ballistics: Examining and interpreting forensic evidence. Second edition. John Wiley & Sons, 2008.
- [4] D. E. Carlucci and S. S. Jacobson, Ballistics: Theory and design of guns and ammunitions. N.Y.: CRC, 2007.
- [5] H. Rebai, „Tribology and machine elements: Mechanical engineering and production technology,“ B. thesis, University of applied sciences. Riihimäki: HAMK, 15.08.2014.
- [6] J. Jain, S. L. Soni and D. Sharma, “Determination of wear rate equation and estimation of residual life of 155 mm autofrettaged gun barrel,” Int. Jnl. of Multiphysics, Volume 5, Number 2011. Available: Research Gate <https://www.researchgate.net/>. [Accessed February 5, 2024].
- [7] J.-s. Ma, „The law of barrel wear and its application,“ Defence Technology, Volume 14, Issue 6, pp. 674-676, December 2018. [Online]. Available: Science Direct, <https://www.sciencedirect.com>. [Accessed February 3, 2024], <https://doi.org/10.1016/j.dt.2018.06.012>
- [8] M. J. Neale, The tribology handbook. Second edition. BH, 2001 г.
- [9] R. C. Juvinall and K. M. Marshek, Fundamentals of machine component design. Fifth Edition. Wiley, 2012.
- [10] R. G. Hasenbein, “Wear and erosion in large caliber gun barrels,“ Defence technical information centre, 2004, [Online]. Available: DTIC, <https://apps.dtic.mil/>. [Accessed February 9, 2024].
- [11] V. Yastrebov and G. Ancaix, Eds., From infinitesimal to full contact between rough surfaces: Evolution of the contact area. HAL, 13.08.2015 г.
- [12] Б. П. Сафонов и А. В. Бегова, Инженерная трибология: Оценка износостойкости и ресурса трибосопрежений. Новомосковск, 2004.
- [13] В. Л. Попов, Механика контактного взаимодействия и физика трения. От нанотрибологии до динамики землетрясений. Москва, 2013.
- [14] Г. Ганев, Р. Лазаров и Б. Банков, “Подход за определяне на балистични характеристики на боеприпасите,“ Сборник доклади от International scientific conference “Defense Technology Forum 2023”, с. 285-289, ISSN 2815-4274, Shumen, 2023, [Онлайн]. Достъпна: DTF, <https://dtf.aadcf.nvu.bg/archives/>.
- [15] Г. С. Здравчева, „Изследване на износоустойчиви покрития, нанесени върху електрохимично обработени детайли“, Дисертационен труд, Технически университет – София, Факултет „Инженерно-педагогически факултет“. Сливен, 2023. [Онлайн]. Достъпна: НАЦИД, <https://nacid.bg>. [Посетено Януари 30, 2024].
- [16] И. И. Беркович и Д. Г. Громаковский, Трибология: Физические основы, механика и технические приложения. Самара, 2000.
- [17] К. Г. Калев, Влияние на изменението на геометрията на канала върху балистичните параметри на оръдейното тяло. Шумен, 2017.
- [18] К. Г. Люцканов, „Изследване влиянието на факторите на абразивното износване при наваряване на детайлите от драгажния флот“, Дисертационен труд, ВВМУ „Никола Йонков Вапцаров“, Факултет „Инженерен“. Варна, 2017. [Онлайн]. Достъпна: НАЦИД, <https://nacid.bg>. [Посетено Януари 30, 2024].
- [19] М. Кандева, Инженерна трибология: Цикъл лекции за докторанти, ТУ-София: МТФ, 2012.
- [20] М. Серебреков, Вътрешна балистика. София, 1996.
- [21] Н. Манолов и М. Кандева, Обща трибология. София, 2004.



# Security analysis of lightweight cryptographic algorithms

**Dilyana Dimitrova**

Department of Information Technologies  
Nikola Vaptsarov Naval Academy  
Varna, Bulgaria  
di.dimitrova@naval-acad.bg

**Ivaylo Dimitrov**

Engineering Department  
Blu11 Ltd.  
Varna, Bulgaria  
ivailo.dimitrov@blu11.com

**Abstract.** The paper examines three lightweight cryptographic algorithms - SKINNY, ForkAE, and Romulus. The research focuses on evaluating their security against various cryptographic attacks. Methods used: theoretical analysis and summary. Results indicate that all three algorithms exhibit strong security properties against common cryptographic attacks. SKINNY stands out for its security even with few encryption rounds, while the presence of SKINNY as a building block in the other two ciphers - ForkAE and Romulus makes them at least as secure as SKINNY.

**Keywords:** *lightweight cryptographic algorithms, lightweight cryptography, security analysis*

## I. INTRODUCTION

In the modern world, the use of small IoT (Internet of Things) devices is becoming increasingly common, aiming to simplify our everyday life. While these devices are useful, their widespread adoption, coupled with the increased risk of cyberattacks, is leading to a growing number of vulnerable devices that are not properly protected against attacks. The weaknesses of IoT devices place a significant risk to both user's health and the protection of their personal data. Therefore, the way this information is protected is crucial, including what security and encryption methods are used when transmitting data from the device to the service-providing servers, as well as how the user's personal information is stored. To make IoT devices more secure, appropriate cryptographic algorithms should be used.

When using IoT devices, conventional cryptographic methods such as the symmetric cryptographic algorithm AES, hashing functions like SHA-256, MD5, as well as other cryptographic security methods such as RSA or ECC (Elliptic Curve Cryptography), do not perform optimally on systems with limited computational power and memory capacity because they occupy too much physical space and processor power, consequently consuming too much power, which is unacceptable for devices with limited capabilities [1], [2]. One of the biggest security threats associated with IoT devices is that even the simplest data collection devices (sensors and

measuring modules) can be vulnerable to cyberattacks. Due to their small size and specific applications, most IoT devices do not have the computational power and capabilities of a server installation or even a personal computer. Therefore, special requirements and limitations related to size, consumption, and data processing speed are introduced for lightweight cryptography [3].

## II. MATERIALS AND METHODS

The paper involved the examination of three lightweight cryptographic algorithms: SKINNY, ForkAE, and Romulus. The study aimed to evaluate the security of these algorithms against various cryptographic attacks. Data collection for the study involved gathering information from existing literature sources, including research papers, conference proceedings, and technical documents related to the selected lightweight cryptographic algorithms. Theoretical analysis and summaries were made based on the information obtained from these sources. Theoretical analysis was performed to assess the security properties of the selected cryptographic algorithms. This involved studying the structure of the selected ciphers, key generation methods, encryption and decryption processes, and susceptibility to common cryptographic attacks such as differential and linear cryptanalysis. A summary of the findings from the theoretical analysis was compiled to provide insights into the security of each cipher. Emphasis was placed assessing the overall robustness of the selected cryptographic algorithms against potential attacks.

In the existing literature sources on the topic, analyses of the security of various lightweight cryptographic algorithms have been conducted. In the study [4] a differential cryptanalysis of the lightweight ciphers SIMON and SIMECK is presented, using nested tree search-based methods, to find high probability differential characteristics for the ciphers. The study [5] provides a comprehensive analysis of 101 existing lightweight algorithms, emphasizing the importance of incorporating secure design components such as substitution and permutation functions to ensure robust security in IoT devices. Selection of lightweight cryptographic algorithms

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8233>

© 2024 Dilyana Dimitrova, Ivaylo Dimitrov. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

for analysis might be done using the Analytical Hierarchy Process [6], [7], [8].

The absence of security studies comparing ciphers SKINNY, ForkAE and Romulus following the literature review underscores the relevance of the issue.

### III. RESULTS AND DISCUSSION

#### A. Selected ciphers

Lightweight cryptographic algorithms could be divided into four main types of primitives - block ciphers, stream ciphers, hash functions, and cryptographic algorithms using elliptic curves as it is shown on figure 1. The factors by which each of them can be analysed include the size of the blocks used, the size of the key used, the number of executable rounds, their structure itself, security against different attacks etc.

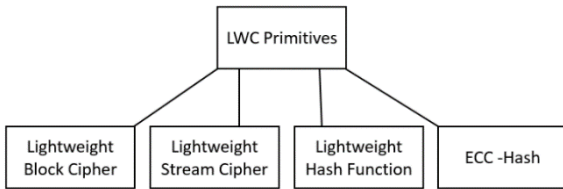


Fig.1. Division of lightweight cryptographic primitives.

The analysed lightweight cryptographic algorithms in the paper are SKINNY, ForkAE, and Romulus.

SKINNY is a lightweight SPN block cipher that uses substitution blocks (S-boxes) [10], as it is shown on fig. 2 [11], a greatly simplified new model for the diffusion layer, and a lightweight method for key generation. The cipher is based on the Tweakable structure, which uses so-called tweakable values [9], [10] as the input key to the cipher, rather than, as in traditional symmetric cryptographic algorithms, a secret key. Essentially, the secret key and the tweakable make no difference in the execution of the cryptographic algorithm.

Representatives of the SKINNY cipher family are SKINNY-AEAD and SKINNY-HASH, which respectively represent an encryption algorithm and a hash function. There are different versions of SKINNY, distinguished by the size of the used data block and the length of the tweakable value. The implementation of SKINNY in an AEAD scheme can be done with both SKINNY-128-256 and SKINNY-128-384 [10], [11]. Both ciphers use data blocks with a size of 128 bits, and the main difference lies in the tweakable value used for the key, with either 256 or 384 bits, respectively.

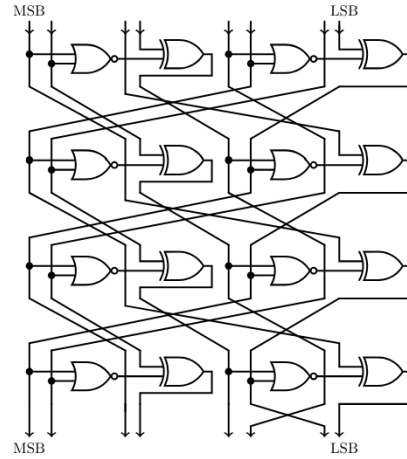


Fig.2. 8-bit S-box construction [11].

ForkAE [12] is a family of lightweight cryptographic algorithms designed to meet the construction of authenticated encryption with associated data (AEAD) ciphers. Unlike SKINNY, ForkAE is tightly optimized for processing short messages. This ensures good performance, security, and simplicity of operation. The cipher's specialization in short messages makes it a suitable candidate for a wide range of lightweight and IoT applications, including wireless sensors, and IoT devices that require very low energy consumption. In addition to these, short messages find applications in critical communication domains of 5G networks and protocols like Bluetooth, where the maximum packet size is 47 bytes.

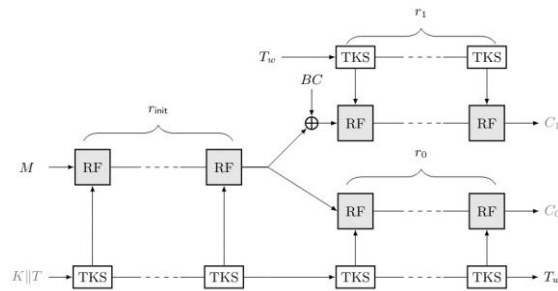


Fig.3. The structure of ForkSkinny, where TKS is round tweakable schedule function and RF is round function [13].

ForkAE is based on a combination of several well-analysed elements [12]. The building block of the cipher is Forkcipher. The standalone use of Forkcipher does not meet the necessary security requirements of NIST. Therefore, to achieve better results, the cipher is combined with another block cipher - SKINNY. This improves efficiency and throughput, as well as revealing new software advantages for applications and better hardware implementations. The combination of the two ciphers is called ForkSKINNY which is shown on fig. 3 [13]. In addition to performance advantages, it provides better results in the field of cryptographic security, as it achieves resistance against a wider range of cryptographic attacks, especially against more modern cryptanalytic techniques.

The security of the cipher depends mostly on round function, so its proper design and use are crucial stages in the design of the specific cipher. The same operations are used to modify the data as SKINNY (SubCells, AddConstants, AddRoundTweakey, ShiftRows,

MixColumns), with the difference that during the "AddConstants" operation, certain changes have been made to the operation's structure. This is because by design, the ForkSKINNY cipher has more rounds than SKINNY, which means that applying the original operation cannot provide the necessary number of unique constants for all rotations of the function. This leads to the repetition of some constant values and can therefore be a vulnerability and weak point in the cipher. The change made by the cryptographers who designed ForkSKINNY to avoid this potential problem is that they increased the length of the constant itself. In SKINNY, the constant has a length of 6 bits, while in ForkSKINNY, it has been changed to 7 bits. This allows the generation of a larger number of unique constant values needed for most rounds in the cipher.

The most significant difference between ForkSKINNY and SKINNY is the presence of an additional step in message processing. This operation is unique to ForkSKINNY, as it is linked to the design and structure of the cipher itself. This step is called forking and is used in generating the two cipher blocks in Forkcipher.

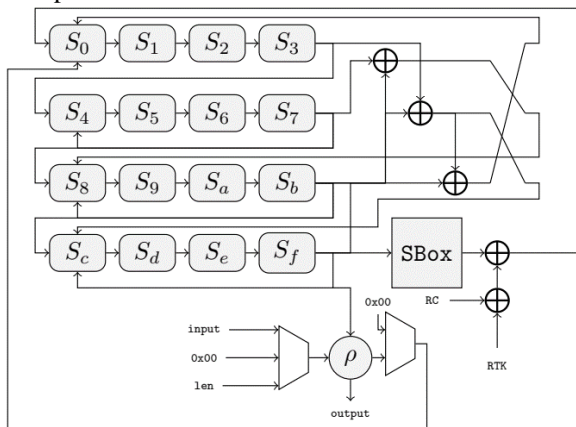


Fig.4. Serial State Update Function used in Romulus [14].

Romulus offers three AEAD schemes - Romulus-N, Romulus-M, and Romulus-T, as well as a hash function - Romulus-H. The cipher is specialized in processing serial data as it is shown on fig. 4 [14]. The first variant of the cipher is oriented towards nonce-based authenticated encryption (NAE). In cryptography, the term "nonce" represents a random number that can only be used once in cryptographic communication. Typically, this number is randomly generated or pseudo-randomly generated, with its primary purpose being to ensure that old communication sessions cannot be reused by an attacker in authenticated encryption. The second variant is applicable for "nonce misuse-resistant" authenticated encryption (MRAE) [14]. The third variant limits the potential for physical data leakage through side-channel attacks. At its core, the Romulus cipher is based on the structure for tweakable block ciphers. The main goal of the cipher is to optimize the NAR/MRAE schemes in such a way that they are applicable in constrained IoT devices.

Like ForkAE, the Romulus team also chose to use the SKINNY lightweight block cipher as the main building block in constructing their cipher. This allows

them to inherit all the strengths of the SKINNY cipher, including all the advancements in cryptographic security achieved by SKINNY. Since SKINNY offers various versions and variants of the used blocks and tweakable values, the Romulus team has opted for only one variant, which features 128-bit blocks and tweakable values of  $2n$  and  $3n$  lengths, meaning 256 and 384-bit values for the tweak.

### B. Cryptographic security

The security of block ciphers, whether they are Feistel ciphers or ciphers based on substitution and permutation, has been extensively studied. However, when the attacker is allowed to have access to encryption or decryption with different keys for the same message, then he can establish various relationships between encryption and decryption operations without knowing the actual message. Many ciphers lose their security and robustness precisely under such attacks. Numerous ciphers considered secure have been compromised by related-key/related-tweak attacks.

The family of block ciphers SKINNY is designed to be resistant to related-key attacks [15], [16]. In this type of attack, the attacker can observe the behaviour of the cipher under different keys without needing to know the initial value of the key used but known mathematical dependencies in its structure [16].

The behaviour of SKINNY against the most well-known attacks in cryptography - differential and linear attacks [15], [17], can be demonstrated by calculating the smallest number of pairs of plaintext and ciphertext for the smallest possible number of active substitution blocks. An active substitution block is defined as any block with a non-zero input difference. Attacks based on differential cryptanalysis exclusively work by detecting differences between input and output data when subjected to some alteration.

Unlike the standard single-key model where the round tweakable keys are constant values and cannot be changed, thus not affecting the activity model, in the related-tweakable model, the attacker can change some of the states of the tweakable matrices. SKINNY can have 3 tweakable input matrices depending on which version of the cipher is being applied, thus there are three attack variants on the tweakable matrices. Only one of the matrices (TK1) may be changed, both at the same time (TK1, TK2), or all three (TK1, TK2, TK3).

The security of the second algorithm - ForkSKINNY, to a certain extent, is based on the security of the SKINNY cipher because it is one of the main building blocks in the overall construction of the ForkAE family of block ciphers [13]. In this regard, all arguments related to the security of SKINNY are applicable here as well. If it is assumed that the attacker has access to the plaintext and at the same time knows the ciphertext of the first block ( $C_0$ ), this type of attack is equivalent to breaking SKINNY with parameters equal to  $r_{init} + r_1$  - round. However, since ForkSKINNY has known structural differences from the original SKINNY and the cipher has an additional forking step on the messages, analysing the security of ForkSKINNY requires an

analysis of the so-called reconstructive attacks. This type of attacks are applicable in situations where the attacker has access to both blocks of ciphertexts and can generate values for one block from the other, and vice versa [18]. This difference in ForkSKINNY is due to the construction of the cipher because the two cipher blocks are interrelated. Reconstructive attacks focus on the middle rounds of the cipher, when operations switch from decryption to encryption.

The last representative of the selected lightweight ciphers – Romulus [19], provides two modes of operation: nonce-respecting (NR) and nonce-misusing (NM). For each of them, there is a proposed value up to which the security of the encrypted data is guaranteed. The security analysis is based on the number of queries made and the total number of processed message blocks. The proposed results guarantee that the cipher is considered secure up to these values and exceeding them could compromise and break the cryptographic algorithm [19]. Table 1 presents the assumed values up to which the Romulus algorithm is considered secure. The numbers in the table represent the effort required by the attacker in terms of data complexity to break the cipher, calculated by taking the logarithm at base 2.

TABLE 1 THE ASSUMED SECURITY VALUES FOR ROMULUS

	Romulus-N	Romulus-M
NR-Priv	128	128
NR-Auth	128	128
NM-Priv	–	64 ~ 128
NM-Auth	–	64 ~ 128

*Meet-in-the-Middle attack*

One way to determine the security of a cipher against Meet-in-the-Middle attacks is to examine the diffusion of the cipher. The diffusion [20] of a cipher represents the number of rounds  $d$ , required for any input bit to influence all other bits of the cipher's internal state (IS) matrix. In other words, the change in one input bit leads to changes in all other bits in the IS matrix. When the key length is equal to the block length and the entire key is used in each round, then for a cipher with diffusion equal to  $d$ , it means that each output bit after that  $d$  round is an expression dependent on all other key bits.

In Meet-in-the-Middle attacks, SKINNY provides very good security [15]. To determine its security level, three important characteristics are considered: partial-matching, initial structure, and splice-and-cut. Each characteristic has a limit at which it may work. For SKINNY, the partial-matching characteristic succeeds up to the 10th round, the initial structure is successful up to the 7th round, and splice-and-cut has been calculated to work up to the 5th round. By combining all characteristics, the number of rounds required for the cipher to withstand Meet-in-the-Middle attacks is obtained. The result is 22 rounds, but SKINNY's capability to operate beyond these 22 rounds, usually 48 or 56, provides significant resilience to this type of attack.

On the other hand, for ForkAE [13], it should be noted that only half of the tweak value is used in each round, and the forking step has a lower diffusion value, which adds additional rounds to the mandatory 22 provided by SKINNY. Thus, the rounds required to break the cipher using a Meet-in-the-Middle attack become even more than 22, indicating that the ForkAE cipher can also be considered resilient to Meet-in-the-Middle attacks.

For the security of the Romulus cipher, specific data regarding its resilience against Meet-in-the-Middle attacks are currently not available. However, considering that Romulus also utilizes SKINNY as its primary building block in its construction, it can be assumed that Romulus is also resilient to Meet-in-the-Middle attacks, at least up to the minimum 22 rounds provided by SKINNY, which are assumed to make the cipher secure.

*Impossible Differential Attack*

In Impossible Differential attacks, two values ( $\alpha, \beta$ ) are considered, determining that for all possible keys, two messages with an XOR difference equal to  $\alpha$  cannot produce other two messages differing by  $\beta$  after a certain number of encryption rounds ( $r$ ) [21]. To discover the key, the attacker adds several rounds before and after  $r$ , then makes assumptions about some key bits, checking if the values for  $\alpha$  and  $\beta$  are confirmed. If so, the assumption about the key is wrong because it leads to an impossible situation (two different keys having the same  $\alpha$  and  $\beta$  values). After a certain number of repetitions, the total number of keys becomes small enough to apply a brute force attack on the key by trying all possible key variants.

The security of SKINNY [15] against this type of attack is evaluated at a maximum of 11 rounds of encryption, beyond which the cipher is considered to be broken if a truncated attack type is used. After these 11 rounds, it is assumed that the key information is lost, and the attack becomes ineffective. If the attacker has access to the relationship between different tweak values (related-tweakey), the security of SKINNY increases with each used tweak value. Accordingly, SKINNY can use 3 tweak value matrices, and depending on the number used, the following security values against Impossible Differential attacks are determined: TK1 (128 bits) - 12 rounds, TK2 (256 bits) - 14 rounds, and for TK3 (384 bits) - 16 rounds.

On the other hand, in ForkAE [13], it is necessary to determine the security during the forking operation because the remaining cipher structure is like SKINNY. However, if the security of the cipher is viewed only during the forking operation, it is like that of SKINNY. It has been calculated that a truncated differential attack is not possible after the 12th round of ForkAE, making it as secure as SKINNY at least.

The security of Romulus depends entirely on the cryptographic security obtained from SKINNY since Romulus does not make significant changes to the design of its underlying cryptographic primitive - SKINNY.

#### IV. CONCLUSIONS

SKINNY is a lightweight Substitution-Permutation Network (SPN) block cipher based on the tweakey structure, which specializes in processing messages in a parallel manner. ForkAE is a family of lightweight block cryptographic algorithms that are closely optimized for processing short messages. Romulus is a block cipher specialized in processing serial data. Each cipher is specialized in a specific direction and offers different modes of operation, authentication methods, and possibilities for software and hardware implementation.

The family of block ciphers SKINNY is designed to be resistant to related-key attacks. SKINNY also demonstrates good resistance against differential and linear attacks. The security of ForkSKINNY to a certain extent is based on the security of the SKINNY cipher. However, its construction has known structural differences from the original SKINNY, making it susceptible to reconstructive attacks. Every cipher has proposed secure values which guarantee that the cipher is considered secure up to these values and exceeding them could compromise and break the cryptographic algorithm.

The security of a cipher against Meet-in-the-Middle attacks can be determined by examining its diffusion. SKINNY provides very good security against Meet-in-the-Middle attacks, with a required number of rounds of 22. The rounds required to break ForkAE with this type of attack are more than this of SKINNY. The Romulus resilience against Meet-in-the-Middle attacks is currently unknown, but since it uses SKINNY as its primary building block, it can be assumed to be resilient up to the minimum 22 rounds required by SKINNY.

The security of SKINNY against Impossible Differential attacks is evaluated up to 11 rounds of encryption, beyond which the cipher is considered to be broken. ForkAE is at least as secure as SKINNY against this type of attack. Romulus's security depends on SKINNY's cryptographic security.

After analyzing the selected lightweight cryptographic algorithms, it can be concluded that the security the ciphers provide against well-known attacks such as differential and linear cryptanalysis, as well as attacks like Meet-in-the-Middle Attack and Impossible Differential Attack, meets current security requirements. The SKINNY cipher offers good security even with a small number of rounds used, and its ability to use a significantly larger number of rounds in its encryption function makes it resistant against the most well-known cryptographic attacks. The presence of SKINNY as a building block in the other two ciphers, ForkAE and Romulus, also makes them at least as secure as SKINNY.

The report is in implementation of the National Scientific Program "Security and Defense", adopted with RMS No. 731/21.10.2021, and financed by the Ministry of Education and Science of the Republic of Bulgaria according to Agreement No. D01-74/19.05.2022.

#### REFERENCES

- [1] W. Easttom, *Modern Cryptography: Applied Mathematics for Encryption and Information Security*. Springer, 2021.
- [2] M. Banday, *Cryptographic Security Solutions for the Internet of Things*. IGI Global, 2019.
- [3] NIST, "Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process" [Online]. Available from: <https://csrc.nist.gov/csrc/media/Projects/lightweight-cryptography/documents/final-lwc-submission-requirements-august2018.pdf>.
- [4] A. D. Dwivedi and G. Srivastava, "Security analysis of lightweight IoT encryption algorithms: SIMON and SIMECK," *Internet Things*, vol. 21, p. 100677. ISSN 2542-6605, 2023. doi:10.1016/J.IOT.2022.100677.
- [5] A. A. Zakaria et al., "Systematic literature review: Trend analysis on the design of lightweight block cipher," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 35, no. 5, p. 101550. ISSN 1319-1578, 2023. doi:10.1016/J.JKSUCI.2023.04.003.
- [6] V. Petrova, "The Hierarchical Decision Model of cybersecurity risk assessment" 12th National Conference with International Participation (ELECTRONICA), vol. 2021, 2021, pp. 1-4. doi:10.1109/ELECTRONICA52725.2021.9513722. 978-1-6654-4061-5.
- [7] V. Petrova, "Using the Analytic Hierarchy Process for LMS selection": 20th International Conference on Computer Systems and Technologies. Ruse, Bulgaria: Pages, ISBN: 978-1-4503-7149-0, Jun. 2019, pp. 332-336. doi:10.1145/3345252.3345297.
- [8] M. Sotirov and V. Petrova, "The Nine-Steps Gamification Process: Increasing Student Engagement in LMS," in *2023 International Conference Automatics and Informatics (ICAI)*, IEEE, 2023, pp. 496-501.
- [9] J. Jean et al., "Tweaks and keys for block ciphers: The TWEAKEY framework" in *Asiacrypt 2014. Lecture Notes in Computer Science*, vol. 8874, P. Sarkar, T. Iwata, Eds. Berlin, Heidelberg: Springer, 2014, 274-288. doi:10.1007/978-3-662-45608-8\_15.
- [10] C. Beierle et al., "The SKINNY family of block ciphers and its low-latency variant MANTIS" in *Crypto 2016. Lecture Notes in Computer Science*, M. Robshaw, J. Katz, Eds., 2016, 123-153. doi:10.1007/978-3-662-53008-5\_5(5), vol 9815. Springer, Berlin, Heidelberg. [https://doi.org/10.1007/978-3-662-53008-5\\_5](https://doi.org/10.1007/978-3-662-53008-5_5).
- [11] C. Beierle et al., "SKINNY-AEAD and SKINNY-Hash v1.1." Accessed: Dec. 11, 2019. [Online]. Available: <https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/SKINNY-spec-round2.pdf>.
- [12] A. Deprez et al., "Optimized software implementations for the lightweight encryption scheme ForkAE" in *Smart Card Research and Advanced Applications*, P. Y. Liardet, N. Mentens, Eds., 2021, 68-83. doi:10.1007/978-3-030-68487-7\_5 Smart Card Research and Advanced Applications. CARDIS, Lecture Notes in Computer Science, 2020(0), vol 12609. Springer, Cham. [https://doi.org/10.1007/978-3-030-68487-7\\_5](https://doi.org/10.1007/978-3-030-68487-7_5).
- [13] E. Andreeva, A. Deprez, J. Pittevels, A. Roy, A. Singh Bhati, and D. Vizár, "New Results and Insights on ForkAE." Accessed: Apr. 17, 2024. [Online]. Available: <https://csrc.nist.gov/CSRC/media/Events/lightweight-cryptography-workshop-2020/documents/papers/new-results-ForkAE-lwc2020.pdf>.
- [14] T. Iwata et al., "Romulus v1.2" [Online]. Available at: <https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/Romulus-spec-round2.pdf>.
- [15] C. Beierle et al., "SKINNY-AEAD and SKINNY-hash v1.1." Available at: <https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/SKINNY-spec-round2.pdf>. NIST [Online].
- [16] R. Ankele et al., "Related-Key Impossible-Differential Attack on Reduced-Round SKINNY." Accessed: Apr. 17, 2024. [Online]. Available: <https://eprint.iacr.org/2016/1127.pdf>.
- [17] H. M. Heys, "A TUTORIAL ON LINEAR AND DIFFERENTIAL CRYPTANALYSIS," *Cryptologia*, vol. 26, no.

- 3, pp. 189–221, Jul. 2002, doi: <https://doi.org/10.1080/0161-110291890885>.
- [18] K. G. Paterson et al., “Security against related randomness attacks via reconstructive extractors” in Lect. Notes Comput. Sci.. IMACC 2015, J. Groth, Ed. Cryptography and Coding, 2015(), vol 9496. Springer, Cham. [https://doi.org/10.1007/978-3-319-27239-9\\_2](https://doi.org/10.1007/978-3-319-27239-9_2).
- [19] C. Guo et al., Final-Round Updates on Romulus, 2022.
- [20] C. Shannon, “Diffusion and Confusion.” Available: <https://www.nku.edu/~christensen/diffusionandconfusion.pdf>.
- [21] A. Biryukov, "Impossible Differential Attack," in Encyclopedia of Cryptography and Security, H.C.A. van Tilborg, Ed. Boston, MA: Springer, 2005, pp. 197. [Online]. Available: [https://doi.org/10.1007/0-387-23483-7\\_197](https://doi.org/10.1007/0-387-23483-7_197).

# Antivirus Performance Evaluation against PowerShell Obfuscated Malware

**Radostin Dimov**

Artillery, AD and CIS Faculty,  
National Military University „V. Levski”,  
Shumen, Bulgaria  
[rsdimov95@gmail.com](mailto:rsdimov95@gmail.com)

**Zhaneta Savova**

Artillery, AD and CIS Faculty,  
National Military University „V. Levski”,  
Shumen, Bulgaria  
[zh.savova@yahoo.com](mailto:zh.savova@yahoo.com)

**Abstract.** In recent years, malware attacks have become increasingly sophisticated, and the methods used by attackers to evade Windows defenses have grown more complex. As a result, detecting and defending against these attacks has become an ever more pressing challenge for security professionals. Despite significant efforts to improve Windows security, attackers continue to find new ways to bypass these defenses and infiltrate systems. The techniques covered in this paper are all currently active and effective at evading Windows defenses. Our findings underscore the need for continued vigilance and the importance of staying up to date with the latest threats and countermeasures.

**Keywords:** AMSI Evasion, Antivirus bypass, Defense Evasion, EDR Evasion, PowerShell Obfuscation, Undetected Payload

## I. INTRODUCTION

With the growing complexity of cybersecurity threats, it is becoming increasingly important to secure computer systems against malicious attacks. One of the most commonly targeted operating systems is Microsoft Windows. As a result, many organizations and security professionals are deploying various defensive measures to protect their systems from malware attacks.

PowerShell (PS) is a powerful scripting language that comes built into Microsoft Windows, making it a popular choice for both defenders and attackers. While PS can be used to implement defensive measures, attackers also leverage its capabilities to evade defenses and compromise Windows systems. PS scripts are highly visible and can be easily detected by antivirus software, but attackers can use obfuscation techniques to hide their scripts and make them more difficult to detect.

This paper examines various PS obfuscation techniques that attackers may use or combine as methods to bypass commonly used antiviruses (AVs) and evade detection. By understanding these techniques, defenders can better protect their systems against malicious attacks that utilize PS. This paper explores how these techniques work and why they are effective. It also provides readers

with a comprehensive understanding of the risks associated with PS scripts and the methods that attackers use to evade windows defenses.

The analysis presented in this paper is based on research and testing, as well as real-world observations of attacks using these techniques. By highlighting these techniques, we hope to contribute to the ongoing effort to improve Windows security and protect against malicious attacks.

The research objective is to evaluate the performance of Antimalware Scan Interface (AMSI) and twelve different AV software against obfuscated PS payloads.

### A. AV Detection Methods

AV software uses a variety of techniques to detect malware:

Signature-based detection - involves scanning files for known malware signatures [1]. When the AV software encounters a file that matches a known signature, it will quarantine or delete the file [2]. However, this kind of detection has some limitations as it is ineffective against new and unknown threats.

Heuristic-based detection – relies on set of rules for analyzing the file to determine whether it is malicious or not [3]. This can include looking for specific patterns in the code or program calls.

Behavior-based detection – involves analyzing the behavior of processes running on a system to detect malicious activity [4]. The AV software monitors the system for suspicious behavior such as the process attempting to communicate with a known malicious IP address or downloading stage from a remote host. If a process exhibits such behavior, it may be flagged as malware [5].

Sandbox Detection – part of behavior-based detection which involves running a file or process in a controlled environment to observe its behavior. The AV software

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8201>

© 2024. Radostin Dimov, Zhaneta Savova. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

creates a virtual sandbox where the file can be executed safely without affecting the rest of the system [6]. By observing the behavior of the file within the sandbox, the AV software can determine whether it is malicious or not [7].

However, in general the AV software is integrated with AMSI which adds another layer of security. If a PS payload performs to successfully bypass the AV static signature detection, it has to handle with the AMSI runtime detection [8]. Explaining how AMSI works and its integration with the AV software is beyond the scope of this research.

### B. AV Evasion key techniques

There are various techniques which can be utilized to bypass different AV solution, but in general we can classify them as follows:

Encoding – technique used to hide the true nature of the malware code from antivirus software. By transforming the code into a different format using a scheme, such as base64 or hexadecimal, the malware can bypass signature-based detection. However, encoding is a reversible process, and this technique is becoming less effective as antivirus software improves its ability to detect and decode encoded malware.

Encryption – uses encryption algorithms such as XOR or Advanced Encryption Standard (AES) to encrypt the payload. After execution the encrypted code is decrypted in memory [9].

Obfuscation – consists of sub techniques for modifying the code of the malware to change its signatures and make it more difficult to detect [10]. This includes modifying/reorganizing the source code, object concatenation, splitting and merging techniques so the new relevant signatures are not flagged as malicious [11].

Packers – tools used by attackers to compress and encrypt executable files to make them harder to analyze by security tools and detect malware. These tools are used to evade detection by antivirus software and other security tools. Packed executables are unpacked at runtime, making it harder for security tools to detect and analyze the original code [12].

Reflective Code Loading – technique used to load code directly into a target process's memory, without creating any files on the disk. Commonly used by stager payloads for in-memory code execution. This allows the malware to evade detection by traditional AV software, which often relies on scanning for malicious files or processes [13].

Sandbox Evasion – techniques used to avoid detection when running in a sandbox (virtualization) environment such as time-based evasion or system checks.

### C. Review of related works

In 2018, Jagsir Singh and Jaswinder Singh [14] have analyzed various obfuscation techniques including code replacement, code reorganization, packing, renaming and encryption. The research also reviewed some of the AV detection mechanisms and highlighted effective countermeasures to detect malware obfuscation techniques.

Another research conducted by Kalogranis [15] evaluated four tools, namely AVET (Antivirus Evasion Tool), peCloack.py, Shellter, and Veil-Evasion, against five of the most popular AV solutions – Avast, Bitdefender, ESET Nod32, McAfee and Avira. The AV products selection was based on the products' market share at that time. The research demonstrated that AVET and Veil Evasion had the best performance.

In 2019, a group of authors evaluated the effectiveness of AV evasion tools against windows platform extending Kalogranis' work in a subsequent research [16]. The authors added the Metasploit payload generator and a new tool – TheFatRat, repeating the same tests used by Kalogranis. In comparison to Kalogranis' research, the results showed that AVET and peCloack.py achieved the best effectiveness against the tested AVs. Of course, we have to keep in mind that some of the tools are still in progress and are updated continuously while the tests were performed in 2019.

Similarly, in [17], the author utilized Metasploit payload generator, Hyperion, TheFatRat, Veil-Evasion and Shellter against six AV platforms. The researcher used and combined multiple techniques during the tests. The results highlight Shellter as the most dangerous tool followed by TheFatRat.

Evaluation of Bitdefender AV against different evasion tools was conducted in [18]. The authors analyzed the mentioned AV as one of the best AV platforms and decided to evaluate the effectiveness of nine different open-source tools against only this AV software. The results showed that Phantom Evasion, Onelinepy and PayGen have the highest percentage evasion score against Bitdefender.

In [19] the authors presented a new packer product – PEzoNG which is successor of PEzor – an existing open-source PE and shellcode packer. However, authors mentioned that PEzoNG is a completely different project from PEzor as they only share a part of the name and the building environment. The framework automates the process of creating undetectable binaries targeting Windows Environment. The new product features custom loader, polymorphic obfuscation, anti-sandbox and anti-analysis evasion mechanisms. The effectiveness of the framework for AV detection is tested against 29 different AV solutions and the product is compared to other similar tools.

Even though several studies have evaluated the defense evasion performance of automated tools that may utilize PS as a feature, this research highlights manual evasion methods which allows attackers to personalize their techniques to the target environment and evade specific detection methods. Manual obfuscation doesn't rely on obfuscation algorithms and adversaries can customize the malware manually, making it harder to detect. Adversaries can use a range of techniques, such as renaming variables, splitting code into multiple functions, adding unnecessary code, and encoding or encrypting the code, to make it more difficult to analyze.

## II. MATERIALS AND METHODS

In this research, a virtual lab is developed using VMware ESXi virtualization software to conduct experiments that evaluate the detection capabilities of



AMSI and twelve different AV software against PS defense evasion techniques. By using a virtual lab, we can simulate real-world attack scenarios and assess the performance of AV software against modern cyber threats. The virtual environment - Fig. 1 consists of 13 virtual machines: a Kali Linux 2023.1 attacker box and twelve fully updated Windows Server 2022 sandboxes each running different AV platform with enabled AMSI services. All virtual machines are connected in a separate subnetwork with an IPv4 address range of 192.168.64.0/24 with the attacker box located at 192.168.64.128/24 and the sandboxes at 192.168.64.131-142/24. The attacker box has an opened Netcat listener on TCP port 4444, which will wait for TCP reverse shell connections while testing the AVs detection capabilities against different obfuscation techniques.

The AV platforms that have been selected have demonstrated their exceptional detection capabilities over

the years. These platforms have consistently provided accurate and reliable protection against various types of threats. The utilized AV programs have been rigorously evaluated and have proven their effectiveness in detecting and mitigating known and emerging threats. Additionally, the platforms have received numerous accolades and recognition from reputable organizations in the cybersecurity industry. Their track record of success and continuous improvement make them a reliable and trustworthy choice for protecting against evolving cyber threats.

For the research objective an initial standard PS reverse shell one-liner payload on Fig.2 is used developed by Nikhil Mittal [20]. The payload is then obfuscated with different techniques (Fig. 3) and distributed to the AV sandboxes.

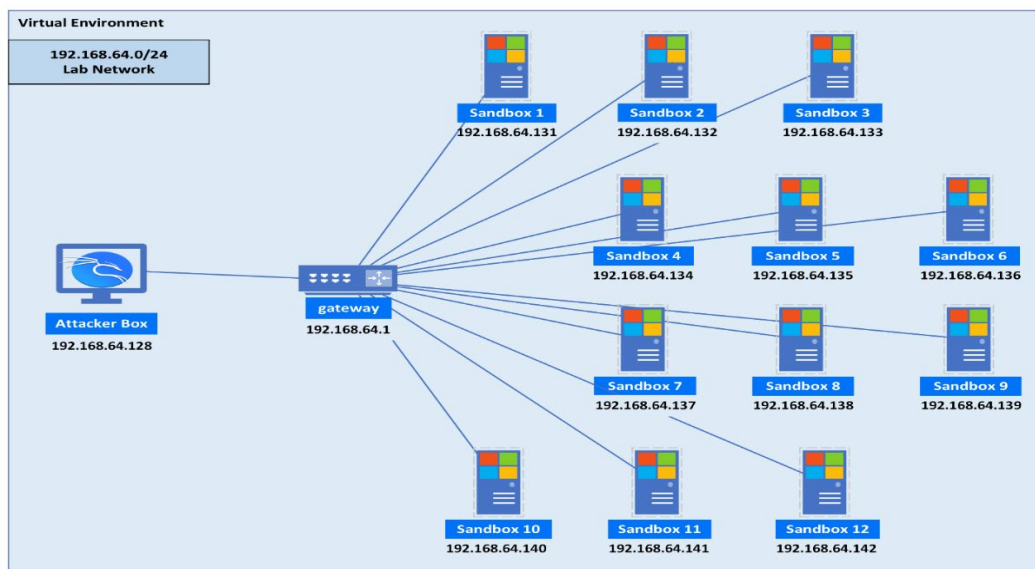


Fig. 1. Experimental network map

```
$client = New-Object System.Net.Sockets.TCPClient('192.168.64.128',4444); $stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2); $stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()
```

Fig. 2. Initial PowerShell Reverse Shell script [20]

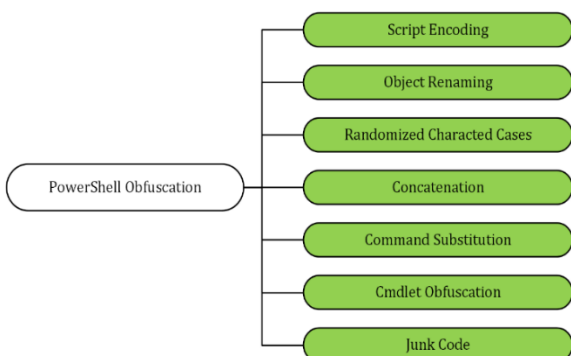


Fig. 3. PowerShell Obfuscation techniques taxonomy

However, as mentioned, AMSI is usually integrated with the AV program which means that we have an additional runtime security layer provided by AMSI. The experimental procedure follows the flowchart on Fig. 4.

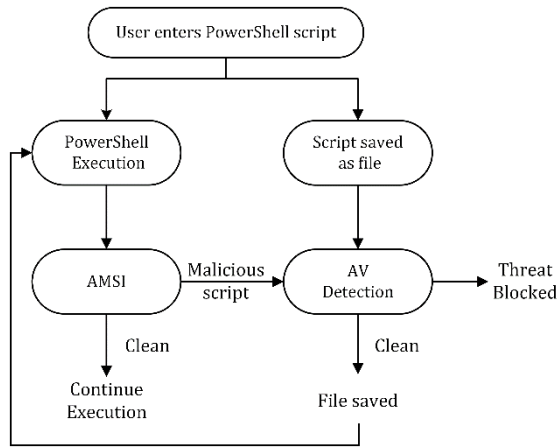


Fig. 4. PowerShell execution flowchart

In the flowchart, there are two paths:

1. If the user enters the PS script directly, it is executed, and the AMSI scans it for malicious code. If the script is not detected as malicious, PS continues the execution. If AMSI detect the code as malicious, an alert is passed through the AV software and script execution is blocked.
2. If the user saves the PS script as a file on the disk, the AV will compare the content of the script file to a predefined database of signatures to identify known malware. If a match is found, the AV software will generate an alert and quarantine or remove the file. If no match is found, the file will remain on the filesystem.

The proposed method can be useful in evaluating the effectiveness of PS manual obfuscation against AMSI runtime detection and AV software for improving their capabilities to detect and prevent attacks that use defense evasion techniques.

Overall, our approach provides a controlled environment for testing AV software and enables us to evaluate their detection capabilities against real-world threats. The findings of this research may contribute to enhancing the effectiveness of AMSI and AV software in protecting against modern cyber threats.

III. RESULTS AND DISCUSSION

If we try to save the script on Fig. 2 on the filesystem as PS script file with .ps1 extension, it will be immediately flagged as malicious by Windows Defender real-time protection. Real-time protection performs a static signature scan against every new file saved in the filesystem. On table 1 are shown the AVs detection results of the tested script file.

TABLE 1 INITIAL REVERSE SHELL DETECTION RESULTS

No	AV Software	Detection
Results collected November 2023		
<b>Static Detection</b>		
1	Microsoft Defender	Detected
2	Avast Antivirus	Detected
3	AVG Anti-Virus	Detected
4	Avira Antivirus	Undetected
5	Bitdefender Total Security	Detected
6	ESET NOD32 Antivirus	Detected
7	Fortinet Antivirus	Undetected
8	Kaspersky Internet Security	Detected
9	McAfee Endpoint Protection	Detected
10	Sophos	Detected
11	Malwarebytes	Undetected

12	Symantec	Detected
Results collected November 2023		<b>Runtime Detection</b>
1	AMSI	Detected

The script is saved as PS file with .ps1 extension and distributed to the AV sandboxes. The results show that the script file is detected by most of the AVs (9/12) either by signature-based detection or heuristic detection. Also, it is detected when executed directly in PS by AMSI. As the script is quite popular and already known to most of the AVs providers, it is also detected as malicious by AMSI. The next experiments perform obfuscation techniques to evaluate the AVs performance and their detection capabilities against PS payload.

A. Encoding (EN)

The proposed experiment aims to evaluate the AVs static signature detection capabilities against encoded PS payloads. The content of the PS Script file – Fig. 2 is base64 encoded with a fixed number of iterations. The encoded payload is then distributed to the AVs sandboxes. After execution the script is decoded in memory. The experiment is repeated with 1, 5, and 10 iterations of base64 encoding the fig. 2 code. The results are presented in table 2. With 10 iterations of encoding, we managed to break 11 of 12 AVs static signatures detection, but not AMSI runtime detection.

As was mentioned earlier encoding is a reversible process. In this example when the encoded script is passed to PS, it is first decoded from base64 and then executed which triggers AMSI runtime detection [21]. An efficient way to bypass AMSI is to encode the strings and decode them within the code [22]. Fig. 5 and 6 shows a brief example where the first command is detected by AMSI as malicious while the encoded one remains undetected.

TABLE 2 BASE64 ENCODING DETECTION RESULTS

No	AV	i=1	i=5	i=10
Results collected November 2023				
<b>Static Detection</b>				
1	Defender	Detected	Detected	Undetected
2	Avast	Undetected	Undetected	Undetected
3	AVG	Undetected	Undetected	Undetected
4	Avira	Undetected	Undetected	Undetected
5	Bitdefender	Detected	Detected	Undetected
6	NOD32	Undetected	Undetected	Undetected
7	Fortinet	Undetected	Undetected	Undetected
8	Kaspersky	Undetected	Undetected	Undetected
9	McAfee	Undetected	Undetected	Undetected
10	Sophos	Detected	Detected	Detected
11	Malwarebytes	Undetected	Undetected	Undetected
12	Symantec	Undetected	Undetected	Undetected
Results collected November 2023				
<b>Runtime Detection</b>				
1	AMSI	Detected	Detected	Detected

```

Invoke-Mimikatz"
# Can be encoded as:
[System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String('SQBuAHYAbwBrAGUALQBNAGkAbQBpAGsAYQB0AHoA'))
  
```

Fig. 5. Encoding Commands

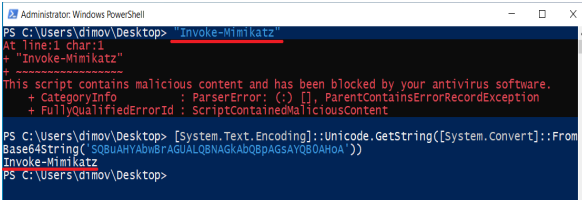


Fig. 6. AMSI Evasion with string encoding

Overall, using base64 encoding, the proposed experiment performed to successfully bypass AVs static signatures detection and provides an effective approach to evade AMSI detection.

**B. Object Renaming (OR)**

A technique which can be utilized for breaking signatures detection and involves changing the names of variables/functions/classes in the code, without changing the functionality of the code itself. This can be done manually or by using tools that automatically rename the objects. Fig. 7 is an example of renaming the variables within the initial PS code on Fig. 2 with low entropy string values. As the script on Fig. 2 contains 8 variables, the experimental results on table 3 evaluate AVs detection capabilities against this technique depending on the number of substituted variables (n).

\$client	\$aaaaaaaaaaaaaaaaaaaaa
\$stream	\$bbbbbbbbbbbbbbbbbbbbb
\$bytes	\$cccccccccccccccccccc
\$i	\$ddddddddddddddddddddd
\$data	\$eeeeeeeeeeeeeeeeeeee
\$sendback	\$fffffffffffffffffffffff
\$sendback2	\$ggggggggggggggggggggg
\$sendbyte	\$hhhhhhhhhhhhhhhhhhhhh
a) Variables	b) Renamed Examples

Fig. 7. Renaming Variables

Substituting all variables within the script results in evading 7 of 12 AVs detection. This technique is also valid for other programming languages such as python, C# or C++. By renaming variables, the malware author can change the "signature" of the code, making it more difficult for AV software to detect. However, AMSI detection is still present. In other words, the script can be saved on the filesystem, but after execution it is detected as malicious by AMSI.

TABLE 3 OBJECT RENAMING DETECTION RESULTS

Nº	AV Software	n=1	n=4	n=8
Results collected November 2023				
<b>Static Detection</b>				
1	Defender	Detected	Undetected	Undetected
2	Avast	Detected	Detected	Undetected
3	AVG	Detected	Detected	Undetected
4	Avira	Undetected	Undetected	Undetected
5	Bitdefender	Detected	Detected	Detected
6	NOD32	Detected	Detected	Detected
7	Fortinet	Undetected	Undetected	Undetected
8	Kaspersky	Detected	Detected	Detected
9	McAfee	Detected	Undetected	Undetected
10	Sophos	Detected	Detected	Detected
11	Malwarebytes	Undetected	Undetected	Undetected
12	Symantec	Detected	Detected	Detected
Results collected November 2023				
<b>Runtime Detection</b>				
1	AMSI	Detected	Detected	Detected

By splitting the script and performing part code execution, we see that the last part of the code – "\$Client.Close()" is triggering the AMSI detection. This doesn't mean that this part of the code is malicious itself, but combined with all the other parts of the script leads to a malicious result.

**C. Randomize character cases (RC)**

This leverages the fact that PS is case-insensitive, meaning that the casing of commands, variables, and arguments does not affect their execution. Exploiting this characteristic, obfuscators introduce variations in character capitalization throughout the code, making it visually distinct from the original form. This alteration disrupts simple string-based pattern matching techniques, as the obfuscated code no longer matches known signatures or standard conventions. The obfuscated code can feature a range of randomizations, including uppercase-to-lowercase, lowercase-to-uppercase, or even selectively mixing capitalization within words or commands [23]. These modifications are applied to specific characters, leaving the overall structure and functionality of the code intact. The goal is to create a visually jumbled representation that evades detection algorithms and human analysis, while still allowing the interpreter to execute the malicious instructions correctly. Fig. 8 represents an example of showcasing the randomization of char cases within a PS code.

iEX Get-Process	iEx "GeT-PrOcEsS"
\$var1="example"	\$vAr1="eXaMplE"
a)Original code	b)Obfuscated code

Fig. 8. Char cases randomization

This method is implemented into the initial PS script code – Fig. 2. Then the updated script is distributed to the AVs sandboxes. The results are shown on table 4. It may look simply but the detection results represent how powerful this technique could be in breaking AVs signatures.

**D. Concatenation (CC)**

Concatenation is the process of combining multiple strings or variables into a single string. This operation is frequently used in PS scripts to create more complex and meaningful output, for example, to construct a custom error message, generate a file path or URL, or format text for display. There are several ways to concatenate strings in PS, including the use of the "+" operator, the "-join" operator, and the string interpolation feature [24]. An example of concatenating strings is shown on Fig. 9.

\$string='192.168.1.121'
\$string='192.16'+ '8.1.121'
\$string='192.1'+ '68.1'+ '.121'
\$string='19'+ '2.16'+ '8.1.1'+ '21'

Fig. 9. String Concatenation

The fourth line of code for example creates a new string by concatenating four separate string literals, '19', '2.16', '8.1.1', and '21'. After the fourth line of code runs, the original value of the \$string variable, '192.168.1.121', is replaced with the concatenated string. The resulting value of \$string is again '192.168.1.121'. A simple concatenation as shown on Fig. 9 is applied into the

strings of the initial script – Fig. 2. AVs detection results for the discussed method are presented in table 4.

*E. Commands Substitution (CS)*

Substituting commands with similar ones that have the same functionality can be used as a technique by malware authors to evade detection by AV systems. By replacing suspicious or known malicious commands with benign or less detectable alternatives, malware can bypass signature-based detection mechanisms and appear innocuous to security software. This technique takes advantage of the vast number of available PS cmdlets and functions that provide similar functionality but have different names or syntax. By using these alternative commands, malware authors can camouflage their malicious activities and make the code less recognizable to AV engines. Fig. 10 provides an example approach in substituting *pwd* cmdlet. This technique allows malware to evade signature-based detections, as the substituted commands do not match known malicious patterns.

```
# Utilizing .NET Framework
[System.IO.Directory]::GetCurrentDirectory()
# Using different cmdlet
Get-Location
# using Get-Location Alias
gl
```

Fig. 10. *pwd* cmdlet substitution example methods

*F. Cmdlet obfuscation (CO)*

In PS, cmdlets can be obfuscated by adding single or double quotes between the characters. The cmdlets can be broken up into multiple segments, and single/double quotes are added around each character. For example, consider the cmdlet *Get-ChildItem*. Using this method, the cmdlet can be broken up into multiple segments, with single or double quotes around each character, as follows:

G'e't-'C'h'i'l'd'i't'e'm

When interpreted by PS, the concatenated example is equivalent to the original cmdlet *Get-ChildItem*. Implementing this technique in the initial reverse shell code – Fig. 2, then the following cmdlets can be substituted with the values shown on Fig. 11. This makes the string harder to read, but again, it is still functional when interpreted by PS [25]. The AVs detection results of the discussed method against the PS code on Fig. 2 are shown on table 4.

```
# iex # Out-String
i'e'x O'u't-S't'r'i'n'g
i''ex Ou"'t-S"tr"i'n"g
i"e"x O'u't-St"r"i'n'g
i''e"x" Ou"'t-'S"'t'r'in'g
i""e'x"" Ou"'t-'S't'r"i'n'g
```

Fig. 11. Cmdlet Obfuscation

TABLE 4 SINGLE TECHNIQUES RESULTS

No	AV	RC	CC	CO
Results collected November 2023				
<b>Static Detection</b>				
1	Win Defender	Undetected	Detected	Undetected
2	Avast	Undetected	Undetected	Undetected
3	AVG	Undetected	Undetected	Undetected
4	Avira	Undetected	Undetected	Undetected
5	Bitdefender	Detected	Detected	Detected

6	NOD32	Detected	Detected	Detected
7	Fortinet	Undetected	Undetected	Undetected
8	Kaspersky	Detected	Detected	Detected
9	McAfee	Undetected	Undetected	Undetected
10	Sophos	Undetected	Detected	Detected
11	Malwarebytes	Undetected	Undetected	Undetected
12	Symantec	Detected	Detected	Detected
Results collected November 2023				
<b>Runtime Detection</b>				
1	AMSI	Detected	Detected	Detected

*G. Adding junk code (JC)*

To evade detection, attackers may intentionally insert extraneous or irrelevant code into their PS payloads. This additional code serves no functional purpose and is designed to confuse or obfuscate the actual malicious commands. By adding junk code, the attackers can make their payloads more difficult for security systems to analyze and identify as malicious. Here’s a brief example:

```
# These lines serve no purpose
# Some irrelevant code
# Actual malicious code
iex "malicious command"
# More unnecessary code
```

Fig. 12. (A) Add Commented-out code block

```
$randomvar1 = "Hello";
$randomvar2 = 123
Function unnecessaryfunc {
    # Irrelevant code
}
# Actual malicious code
iex "malicious command"
```

(B) Add unnecessary variables and/or functions

```
Sleep 0.1; sleep 0.2;
iex "malicious command";
sleep 0.3
```

(C) Add unnecessary sleep timers

```
Get-Process | Out-Null;
Get-Date | Out-Null;
iex "malicious command"
```

(D) Add unrelated function calls

These examples illustrate how junk code can be introduced to PS payloads, making it more challenging for security systems to identify and analyze the actual malicious commands. However, it's important to note that these evasion techniques can vary widely depending on the specific context and objectives of the attacker.

*H. Summary – Putting all together*

The following experiment integrates several techniques outlined in sections A to G, incorporating them directly into the initial PS script – Fig. 2. By utilizing different combinations, malware authors can tailor their obfuscation strategy based on their specific goals and the anticipated defense mechanisms they aim to bypass. The resulting outcomes are presented in table 5. The combined techniques aim to enhance malware obfuscation and evasion capabilities in various ways. The results show that script execution can successfully establish TCP session with an attacker and bypasses AMSI runtime detection as shown on Fig. 13. Table 5

provides a comprehensive overview of the effectiveness and impact of each technique when combined with another. Note that the purpose of the research was to evaluate the effectiveness of the discussed techniques in terms of detection evasion, code obfuscation, and overall

impact on the detection rate of AV systems. By combining these techniques, the experiment sought to demonstrate the potential of employing multiple obfuscation strategies to increase the resilience of PS-based malware against detection and analysis.

TABLE 5 INTEGRATING ALL TECHNIQUES RESULTS

№	AV Software	OR+RC	OR+RC+CC	OR+RC+CC+CS	OR+RC+CC+CS+CO	OR+RC+CC+CS+CO+JC	EN+OR+RC+CC+CS+CO+JC
Results collected November 2023							
<b>Static Detection</b>							
1	Microsoft Defender	Undetected	Undetected	Undetected	Undetected	Undetected	Undetected
2	Avast	Undetected	Undetected	Undetected	Undetected	Undetected	Undetected
3	AVG	Undetected	Undetected	Undetected	Undetected	Undetected	Undetected
4	Avira Antivirus	Undetected	Undetected	Undetected	Undetected	Undetected	Undetected
5	Bitdefender	Detected	Detected	Detected	Undetected	Undetected	Undetected
6	ESET NOD32	Detected	Detected	Detected	Detected	Detected	Undetected
7	Fortinet	Undetected	Undetected	Undetected	Undetected	Undetected	Undetected
8	Kaspersky Antivirus	Detected	Detected	Detected	Undetected	Undetected	Undetected
9	McAfee	Undetected	Undetected	Undetected	Undetected	Undetected	Undetected
10	Sophos	Undetected	Undetected	Undetected	Undetected	Undetected	Undetected
11	Malwarebytes	Undetected	Undetected	Undetected	Undetected	Undetected	Undetected
12	Symantec	Detected	Detected	Detected	Detected	Undetected	Undetected
Results collected November 2023							
<b>Runtime Detection</b>							
1	AMSI	Detected	Detected	Undetected	Undetected	Undetected	Undetected

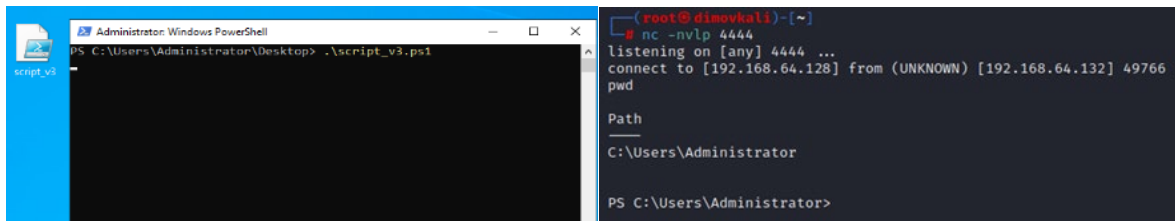


Fig. 13. (A) Script Execution

(B) Session Establishment

#### IV. CONCLUSIONS

In conclusion, this research paper examined different obfuscation techniques employed in PS malware and their impact in AV detection. A virtual environment lab was prepared emulating an attacker box and malware distribution against 12 different AV sandboxes. At the time that these tests were performed, ESET NOD32 demonstrated the best performance among the discussed obfuscation techniques, followed by Symantec. However, as manual obfuscation does not rely on algorithms, it is important to note that the overall effectiveness of the AV systems strongly depends on the specific implementation of these techniques within the malicious script. Notwithstanding, the gathered results may still change over time as AVs signatures are frequently updated to detect new and changed payloads.

The findings showcased that utilizing a single obfuscating technique does not necessarily affect AV detection capabilities. On the other hand, the integration of multiple obfuscation techniques significantly enhance the malware's evasion capabilities resulting in a reduced detection rate and increased difficulty in analyzing the malicious code. These results highlight that the recommended approach in breaking both static-signature detection and runtime detection is by combining different obfuscation techniques, particularly in the context of red team activities.

Moving forward, future research could focus on exploring new obfuscation techniques and developing different detection methods to counter emerging threats.

Additionally, continued collaboration between academia and industry will be crucial in advancing cybersecurity.

#### ACKNOWLEDGEMENTS

This publication was prepared in fulfillment of National Scientific Program – Security and Defense, financed by the Ministry of Education and Science of the Republic of Bulgaria.

#### REFERENCES

- [1] P. Shijo and A. Salim, "Integrated Static and Dynamic Analysis for Malware Detection," in *International Conference on Information and Communication Technologies*, 2015.
- [2] A. B. Ajmal, A. Anjum, A. Anjum and M. A. Khan, "Novel Approach for Concealing Penetration Testing Payloads Using Data Privacy Obfuscation Techniques," in *IEEE 18th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET)*, Karachi, Pakistan, 2021.
- [3] F. Pecorelli, F. Palomba, D. D. Nucci and A. D. Lucia, "Comparing Heuristic and Machine Learning Approaches for Metric-Based Code Smell Detection," in *IEEE/ACM 27th International Conference on Program Comprehension (ICPC)*, Montreal, QC, Canada, 2019.
- [4] Ö. Aslan and R. Samet, "A Comprehensive Review on Malware Detection Approaches," *IEEE Access*, vol. vol. 8, pp. 6249-6271, 2020.
- [5] M. J. e. a. Faruk, "Malware Detection and Prevention using Artificial Intelligence Techniques," in *IEEE International Conference on Big Data (Big Data)*, Orlando, FL, USA, 2021.
- [6] A. Sharma, B. B. Gupta, A. K. Singh and V. Saraswat, "Orchestration of APT malware evasive manoeuvres employed for eluding anti-virus and sandbox defense," *Computers & Security*, vol. Volume 115, 2022.

- [7] N. Miramirkhani, M. Appini, N. Nikiforakis and M. Polychronakis, "Spotless Sandboxes: Evading Malware Analysis Systems Using Wear-and-Tear Artifacts," in *IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, 2017.
- [8] D. Hendler, S. Kels and A. Rubin, "Detecting Malicious PowerShell Commands using Deep Neural Networks," in *ASIACCS '18: Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, 2018.
- [9] A. Al-Hakimi and A. Bakar Md Sultan, "Hybrid Obfuscation of Encryption," IntechOpen, 2023.
- [10] K. Oosthoek and C. Doerr, "SoK: ATT&CK Techniques and Trends in," in *In: Chen, S., Choo, K.K., Fu, X., Lou, W., Mohaisen, A. (eds) Security and Privacy in Communication Networks SecureComm 2019*, 2019.
- [11] H. Xu, Y. Zhou and J. Ming, "Layered obfuscation: a taxonomy of software obfuscation techniques for layered security," *Cybersecurity* 3, 9, 2020.
- [12] O. Or-Meir, N. Nissim, Y. Elovici and L. Rokach, "Dynamic Malware Analysis in the Modern Era—A State of the Art Survey," *ACM Computing Surveys*, vol. vol. 52, 2019.
- [13] Sudhakar and S. Kumar, "An emerging threat Fileless malware: a survey and research challenges," *Cybersecurity* 3, 1, 2020.
- [14] J. Singh and J. Singh, "Challenge of Malware Analysis: Malware obfuscation Techniques," *International Journal of Information Security Science*, vol. 7, no. 3, pp. 100-110, September 2018.
- [15] C. Kalogranis, *AntiVirus Software Evasion: An Evaluation of the AV Evasion Tools*. Ph.D. Thesis, Piraeus, Greece,: University of Piraeus, Department of Digital Systems, 2018.
- [16] S. Aminu, Z. Sufyanu, T. Sani and A. Idris, "Evaluating the effectiveness of antivirus evasion tools against windows platform," *FUDMA Journal of Sciences Vol. 4 No. 1*, pp. 89-92, 2020.
- [17] D. Samociuk, "Antivirus Evasion Methods in Modern Operating Systems," *Applied Sciences*, vol. 13(8):5083, 2023.
- [18] F. Garba, F. Yarima, K. Kunya, F. Abdullahi, A. Bello, A. Abba and A. Musa, "Evaluating Antivirus Evasion Tools AgainstBitdefender Antivirus," in *In Proceedings of the International Conference on FINTECH Opportunities and Challenges*, Karachi, Pakistan, 2021.
- [19] G. D. C. D. & B. G. Bernardinetti, "PEzoNG: Advanced Packer For Automated Evasion On Windows.," *Journal of Computer Virology and Hacking Techniques* 18, p. 315–331, 2022.
- [20] N. S. Mittal, "week of powershell shells day 1," May 2015. [Online]. Available: <http://www.labofapenetrationtester.com/2015/05/week-of-powershell-shells-day-1.html>. [Accessed July 2023].
- [21] D. Hendler, S. Kels and A. Rubin, "AMSI-Based Detection of Malicious PowerShell Code Using Contextual Embeddings," in *In Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (ASIA CCS '20)*, New York, NY, 2020.
- [22] M. Mimura and Y. Tajir, "Static detection of malicious PowerShell based on word embeddings," *Internet of Things*, vol. Volume 15, 2021.
- [23] D. Ugarte, D. Maiorca, F. Cara and G. Giacinto, "PowerDrive: Accurate De-obfuscation and Analysis of PowerShell Malware.," in *In: Perdisci, R., Maurice, C., Giacinto, G., Almgren, M. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment DIMVA*, 2019.
- [24] J. Klasmark, *Detecting PowerShell Obfuscation Techniques using Natural Language Processing*, Dissertation, KTH Royal Institute of Technology, 2022.
- [25] A. Rousseau, "Hijacking .NET to Defend PowerShell," *Malware Research and Threat Intel*, 2017.

# *The Genesis of the Criminal's Personality in the Digital Age*

**Jelena Djubina**  
Riga Stradiņš University  
Riga, Latvia  
[064676@rsu.edu.lv](mailto:064676@rsu.edu.lv)

**Abstract.** The aim of this research is to analyze and understand the issues of a criminal's personality in the digital age to promote more effective crime prevention. It aims to analyze contemporary problems and challenges related to the identification of criminal individuals in the context of digital technologies. This research can contribute to criminology, sociology, and psychology by elucidating how the use of such technology can impact the fight against criminally inclined individuals through digital identification means. The tasks of the research involve analyzing the influence of the digital era on the genesis of a criminal's personality in the mechanism of criminal acts. The novelty of the research is linked to the concentration of the crime prevention system on exploring the mechanism of forming a criminal's personality in the digital age. The research approach will enable a deeper understanding of how the digital era influences the potential formation of personality. The research will employ methods such as theoretical methods based on the analysis of scientific research and publications, exploration of criminal identification processes in the field of digital technology, and the use of content analysis to assess the effectiveness of applied identification technologies. The author assumes that digital technologies provide powerful tools for identifying criminals but are associated with several legal issues. A balance between the use of digital technology, the effectiveness of appropriate methods, and respect for human rights and freedoms is crucial. Recommendations will be provided in the conclusion, focusing on improving legal regulations for identification technologies, considering the identified problems. An analysis of the effectiveness of existing methods and technologies will also be conducted, addressing ethical and legal issues. A special training program and implementation procedure for law enforcement agencies on the ethical and legal aspects of using digital identification methods will be proposed.

**Keywords:** cybercrime, digital crime, genesis, prevention.

## I. INTRODUCTION

The research into the causes of crime, as influenced by the interplay of personality, society, and the environment, integrates into criminology—an interdisciplinary science that melds sociological and legal perspectives. This multifaceted approach

not only enriches criminology with fresh insights but also lays the groundwork for future explorations in the field.

The development of unique theoretical and practical crime monitoring methods, including an interdisciplinary socio-legal methodology alongside modern data analysis techniques, aims to enhance the scientific and practical facets of crime data systematization. These innovations further the advancement of contemporary crime theory and its prevention strategies.

The advent of new technologies brings with it a plethora of ethical dilemmas, from their development to the unforeseeable outcomes of their deployment and the societal impact therein. Computer technologies, in particular, endow society with new possibilities and capabilities previously unattainable. Such technological breakthroughs compel society to contemplate adjustments to regulatory frameworks, to adapt to novel situations brought about by these technologies, and to aptly incorporate new terminologies into practice.

In the digital age, the rapid evolution of technology prompts a societal reevaluation of established viewpoints. The ease and speed with which data can now be exchanged globally, the heightened potential for anonymity, the ability to obliterate electronic materials, and software technologies that facilitate the concealment of one's digital footprint all contribute to a scenario where criminals can operate undetected. The onset of the information and digital technology era necessitates a reexamination of the foundational concepts that shape the criminal personality, underscoring the need for an interdisciplinary approach. The objective of this research is to amalgamate scientific data (research), conduct legal studies, process law enforcement information, and integrate insights from sociology, aesthetics, and ethics, presenting a comprehensive analysis of the challenges at the intersection of technology and criminology.

## II. METHODS

Particular attention is devoted to employing modern methods and technologies in combating crime, alongside pinpointing the limitations and ethical quandaries emanating from the use of digital identification tools. The research employs the following research methodologies: Literature review: This entails a thorough analysis of contemporary scientific research and

Print ISSN 1691-5402  
Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8189>

© 2024 Jelena Djubina. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

publications focusing on cybercrime and the digital identification of criminals. This review provides foundational knowledge and situates the research within the current scholarly discourse [1]. Empirical methods: These involve the collection and analysis of data regarding existing identification technologies, assessing their effectiveness, and identifying issues linked to their application. This method grounds the research in practical, real-world technology applications and their implications [1]. The research also incorporates monographic, analytical, and documentary methods of analysis, alongside the interpretation of legal norms and concepts related to cybercrimes. Utilizing these methods offers a comprehensive understanding of the topic at hand, furnishing objective and valuable insights while ensuring a multifaceted approach [1]. Document and data analysis facilitate the classification and categorization of criminal individuals and the mechanisms of their formation. This process helps in identifying common characteristics and emerging trends. Qualitative data analysis enables the drawing of conclusions from various data sets, including historical events and/or social circumstances, thus providing a nuanced understanding of the factors contributing to the development of criminally inclined personalities. Furthermore, an evaluation of the efficacy of current methods and technologies is undertaken. This evaluation aims to highlight ethical and legal issues related to digital identity, offering a holistic view of the challenges faced in the digital age. By integrating these diverse methods, the research aims to contribute significantly to the fields of criminology and digital ethics, proposing solutions that balance technological advancements with ethical considerations and legal compliance.

### III. MATERIALS

On the official website of the European Union Agency for Criminal Justice Cooperation (Eurojust) [8], cybercrime is defined as a growing and fast-evolving crime area, which accounts for a substantial share of Eurojust's overall casework [8]. The growing overlap between crimes originating on the Internet and cyber-enabled crimes such as terrorism and money laundering poses significant challenges for law enforcement agencies in tracking and apprehending cybercriminals [8]. This includes the loss of electronic data crucial for successful cybercrime investigations, the difficulty in locating perpetrators who actively conceal their physical whereabouts, legal ambiguities, and the lack of specific regulations aimed at preventing digital criminal activities. Furthermore, differences in the legal frameworks among EU member states often present serious obstacles to international cybercrime investigations, and there is no common legal basis for expedited evidence exchange.

Analyzing scientific research conducted in Nigeria, scholars describe a very high youth population, which constitutes more than 70% of Nigeria's total population, and a high level of unemployment. Youth who are not studying or working contribute to the rise in crime, especially in the growing level of cybercrime. Cybercrimes, such as fraudulent electronic mails, identity theft, hacking, cyber harassment, spamming, and Automated Teller Machine spoofing, are more prevalent in Nigeria than other types of crimes, locally referred to as "Yahoo Yahoo" [4]. In 2020, internet fraud crimes, such as online romance scams, interception of business transactions for fraud purposes, hacking of government and private bank accounts, and fraudulent investment schemes, were widespread. These crimes have been gaining momentum since 2000, with the advent of the internet, computers, and mobile phones. By 2020, Nigeria had become a "hotspot," ranking third in global internet crime rates [4].

Cybercrime is defined as any unlawful behavior directed at compromising the security of computer systems and the data they process, or any unlawful behavior committed through or

against computer systems or networks [4]. Youth feel empowered and unpunished in this realm, demonstrating their wealth acquired through criminal means, enticing new recruits into this criminal business, and showing them how to quickly become wealthy without exerting any effort. Youth rapidly and adeptly acquire computer technologies and internet skills, mastering cyberspace to explore its opportunities and understand the legality of their actions. Once they realize that their illegal activities lead to quick monetary gains, they become engrossed in the process, remaining unemployed but contributing to the increase in crime. Cybercrimes are more characteristic of youth, as they quickly acquire digital literacy combined with readily available hacking tools [4]. Young unemployed graduates or high school dropouts, living in poor socio-economic conditions, mainly participate in internet frauds. They lack motivation to pursue education due to financial constraints and view computer fraud as an alternative means of livelihood. To become internet fraudsters, all one needs is a computer, phone, and internet connection, and youth are taught these skills by those already involved in such crimes. This rapid learning of internet fraud basics is termed "web freestyle" [4].

Due to high unemployment and rapidly increasing crimes, Nigerian authorities have decided to increase job opportunities in the private sector that align with youths' knowledge and skills in computer technologies, redirecting youth intellect away from criminal activities. However, scholars have also acknowledged that the consequences of youth unemployment amidst the rise in cybercrimes among Nigeria's youth have not been adequately studied. Therefore, it was decided to conduct deeper research on this issue to identify the impact of youth unemployment on the cybercrime threat in Nigeria.

Delving into theory, in countries where youth constitute a significant portion of the population, the population often faces youth unemployment, making them more vulnerable to recruitment into various terrorist and criminal groups prone to violence and crimes associated with the large youth population. In countries with a large youth population neglected by authorities, crime, led by youth, tends to rise. The Nigerian government must strive to ensure that the country's youth contribute positively to society. This situation indicates that cybercrime has become a profitable enterprise and an alternative source of income for unemployed youth.

In Italy, there is a notably high level of cybercrime, particularly cyberbullying. Cyberbullying encompasses various forms of electronic aggression, harassment, blackmail, insult, humiliation, defamation, theft or alteration of personal data, illegal acquisition of such data, manipulation, and damage to personal data of minors [2]. Additionally, individuals in cyberspace have learned to spread online content aimed at minors or their family members. The goal of distributing such content is to deliberately tarnish and isolate the minor or group of minors, exposing them to serious violence, harm from attacks, or mockery [2]. The internet serves as a powerful tool for criminally inclined individuals to commit property-related offenses such as fraud, theft, money laundering, and to engage in illegal activities, including human trafficking, with organized crime adapting its methods from the real world to cyberspace. In the financial-economic sector, cybercrime includes so-called "white-collar" crimes.

The Italian State Police attempted to outline the profile of the cyber-criminal, identifying him as "a non-violent subject, with a low need to contain anxiety, determined by the fact that the crime does not take place in a physical place, strictly contact with the victim, but in the digital environment" (Lorusso, 2011) [2]. This detachment allows the criminal not to identify with a criminal persona and, consequently, not to associate their actions with crimes. Furthermore, Italian legislation includes an article providing punishment for cyberstalking, seen as the digital equivalent of the crime of persecution [2]. The article has been



reinforced with stricter punishment measures if the crime is committed using IT tools such as email, SMS, malware, and social networks. Psychology identifies several profiles of stalkers: 1) The resentful, who seeks revenge for a partner's abandonment through repeated persecutory conduct; 2) The affection seeker, who attempts to establish a friendly, dependent relationship, often found in patient-doctor contexts; 3) The incompetent suitor, who may start as a work or university colleague and becomes persistently annoying through unwanted attention; 4) The rejected, who, after refusal from an ex-partner or suitor, tries persistently to maintain any form of relationship; 5) The predator, one of the most violent types, whose desire is solely sexual, planning and hunting their victim [2]. The emergence of the internet introduced the cyberstalked, a sophisticated type of stalker who influences their victim remotely, via information technologies, thus widening the gap between the criminal and their victim. This capability allows the criminal to transcend physical boundaries; they do not physically touch the victim and lack any feelings of compassion towards them. Additionally, in Italy, cybercrimes such as "online revenge," involving the illegal distribution of sexually explicit images and videos, are prevalent, with punishment measures also being tightened [2].

Researchers have conducted an analysis of risk factors for juvenile cybercrime, focusing not on traditional crimes but on cybercrimes such as hacking attacks and sexting committed by minors. In these studies, hacking is considered a form of cyber-dependent criminal activity, whereas cyberbullying and sexting are viewed as forms of criminal behavior involving cybersecurity [5]. For various types of cybercriminal behavior, it has been found that perpetrators demonstrate relatively low internal moral and social values. Similar to traditional crimes committed by minors, cybercrimes have identified risk factors such as peer influence on deviant behavior among minors, directed towards cyberbullying and hacking, as well as peer pressure directed towards sexting. Significant risk factors for cyberbullying included prior offenses and victimization in both online and offline environments. Additionally, the influence of the dark web, especially in cyberbullying, and a very high level of computer addiction were identified. Studies have shown that these risk factors were mitigated among minors attending middle or high school. However, to draw accurate conclusions, further in-depth research is needed.

#### IV. RESULTS AND DISCUSSION

Cybercrime is distinguished by the fact that cybercriminals do not necessarily need to be physically present at the scene of the crime. It refers to "a crime in which the behavior or material object of the crime is connected to IT or telematic systems, i.e., software that receives data, for example, from mobile devices and displays it on a computer or smartphone screen, or is committed using such a system" [2]. Due to the rapid growth of various types of cybercrimes, changes have been made to Italian legislation, particularly to the Penal Code, to increase punishments for actions where crimes are committed using information technology tools. These changes provide legal grounds for prosecuting the illegal distribution of sexually explicit materials, images, and videos. Analyzing various studies, it can be concluded that the criminological assessment of criminal behavior should consider the influence of virtual space on the cognitive processes of criminal personalities. Cybercrime significantly differs from traditional crime and undoubtedly requires special and ongoing attention in the field of criminological research.

Researchers in the USA have proposed their own methodology for tracking criminals committing crimes in

cyberspace. This methodology is based on the mathematical concepts of identification codes, ensuring a reduction in resources from law enforcement agencies without compromising the ability to unambiguously identify a suspect when they become "active" in activities related to terrorism or narcotics. This method operates under the assumption that when an individual becomes "active" in drug trafficking or human trafficking activities, their friends/accomplices will have some knowledge of their individual plan. Accordingly, even if an individual is not under direct surveillance by law enforcement agencies (such as phone call records, movements, social interactions with others) but is on the list of friends/accomplices of the person involved in drug-related activities, those involved in drug-related activities can be unambiguously identified [3].

With increasing attention, research on the Dark Tetrad (D4) is gaining momentum [7]. The Dark Tetrad encompasses a set of personality traits that combine negative characteristics such as narcissism, Machiavellianism, psychopathy, and sadism. These traits share common features, including a lack of empathy and low agreeableness towards others. Machiavellianism is characterized by selfishness, a tendency towards manipulation, and motivation to exploit others. Narcissism is defined by a strong sense of self-worth, presumed superiority, and interpersonal domination. Individuals displaying psychopathic traits often exhibit impulsiveness and are inclined towards sensation-seeking and antisocial behavior. Those with sadistic inclinations derive pleasure from intentionally inflicting psychological and physical pain on others [7]. Consequently, relationships with individuals exhibiting heightened D4 traits can be problematic and pose risks to the physical and emotional well-being of those interacting with them.

Individuals with elevated D4 traits show a greater propensity for cyberstalking intimate partners, monitoring their behavior, phones/computers, or using apps to observe their activities, with sadistic tendencies being a primary indicator of such behavior. Online platforms, where individuals can seek new and short-lived acquaintances to satisfy their goals and needs, are highly characteristic of individuals with elevated levels of D4 traits. However, scientists cannot definitively say whether people with elevated D4 traits prefer online searches or offline encounters. They advise society to be cautious in choosing dating partners and to identify individuals with heightened D4 traits at an early stage to avoid potential victimization.

With the rapid advancement of information technology, particularly the significant growth in computer gaming, society is witnessing a rise in aggression and criminal behavior among individuals, primarily impacting the younger generation. Various studies have shown that children engrossed in computer games become aggressive and antisocial, leading to the development of criminal personality traits. Many psychologists argue that computer games with aggressive content cultivate an aggressive and destructive behavioral pattern in individuals. In many computer games, adolescents can engage in actions that are socially disapproved, providing them with emotional release that they cannot find in their external environment. Computer games often include auditory signals, which also exert additional psychological influence, potentially even provoking psychological disorders [6]. Furthermore, such auditory signals, when encountered in the external environment, can trigger bursts of aggression, which could serve as a catalyst for the commission of violent criminal offenses, including causing grievous bodily harm and even murder.

As minors often exhibit heightened emotional arousal, which quickly escalates into aggression and mental instability, leading to affective outbursts, they are susceptible to the influence of external factors and experienced criminals, as well as groups such as terrorists and drug-related entities. These groups easily

persuade minors to engage in unlawful activities, presenting a significant problem at present.

## V. CONCLUSIONS

With the rapid development of digital technologies, society has witnessed a decline in humanity and empathy, leading to an increase in virtual relationships. The cyber realm offers an opportunity for criminally inclined individuals to commit illegal actions with confidence in remaining unpunished. The high level of criminal activity facilitated by the internet has prompted legislators to swiftly respond with effective amendments to legislative acts, aiming to prevent the dangers posed by cyberspace and its influence on the world at large. Given that cybercrime significantly differs from conventional crime, studies must consider the influence of virtual space on the cognitive processes of criminally inclined individuals, such as acquiring new knowledge and making appropriate decisions. These processes involve various cognitive functions that aid in acquiring knowledge and understanding the surrounding world, including perception, attention, memory, and reasoning.

In a world where digital technologies are rapidly advancing, constructing a criminological profile of offenders, whose activities are geared towards property crimes or crimes against individuals, proves challenging. It is difficult to establish the behavior of such criminals, their physique, the clothing they wore at the time of committing any cybercrime, and also to determine the psychological profile of the offender. Virtual reality allows criminals to blend in, as cyberspace lacks a clear description of appearance, emotions, or feelings. Moreover, individuals committing cybercrimes likely experience emotional inadequacy and seek compensation specifically within cyberspace, where they can affirm themselves and receive recognition from strangers. Perhaps, to reduce cybercrime, society needs to engage schoolchildren in various clubs and sports sections, and involve students in cultural and mass work to prevent them from constantly being in cyberspace and to deter the temptation to commit cybercrimes.

In conclusion, it remains a fact that only specific individuals commit criminal offenses. Understanding what happens at their psychological and biological levels is crucial for studying the criminal's personality to subsequently reduce the likelihood of criminal offenses. Major global organizations such as The International Criminal Police Organization (Interpol), The United Nations Office on Drugs and Crime (UNODC), and Drug Trafficking Organizations (DTO) have developed methodologies aimed at activities related to drug trafficking or terrorist groups in cyberspace. These organizations analyzed judges' comments on verdicts, created a network of individuals involved in drug distribution, studied the network of drug-related criminals, analyzed court transcripts, and identified key participants to create a social network. These combined actions yielded positive results for further tracking individuals involved in terrorist groups and drug trafficking. If such coordinated efforts are applied in countries where the number of various cybercrimes is rapidly increasing, it is my view that fruitful results will be achieved in the near future.

Additionally, it is worth noting that in practice, it is very difficult to consider all the factors that can become causes and lead to the commission of criminal offenses. Therefore, one of the main tasks before science is to identify the determinants for specific criminal offenses, namely to identify the causes and conditions of the crime.

## REFERENCES

- [1] K.Martinson and A.Piper. "Methodology of scientific activity: an interdisciplinary perspective". Riga, RSU, pages 608. 2021.
- [2] F.Greco; G.Greco. "INVESTIGATIVE TECHNIQUES IN THE DIGITAL AGE: CYBERCRIME AND CRIMINAL PROFILING". European Journal of Social Sciences Studies. June 2020. DOI: 10.5281/zenodo.3877668
- [3] K.Basu, A.Sen. "Social Networks. Identifying individuals associated with organized criminal networks: A social network analysis". NetXT Lab, School of Computing, Informatics and Decision Systems Engineering, Arizona State University, 699, South Mill Ave., Tempe, AZ, USA. Jan 2021.
- [4] Obianagwa, Christopher Ewuzie; Ngoka Ruth Obioma; Gift, Uwaechia Onyinye; Hayford, Ezugwu Ikechukwu; Okpala Joy Chinaza; et al. "Youth Unemployment and Cybercrime in Nigeria". African Renaissance; London. United Kingdom Vol. 20, Iss. 2, 177–199. Jun 2023. DOI:10.31920/2516-5305/2023/20n2a9
- [5] Inge B. Wissink, Joyce C.A. Standaert, Geert Jan J.M. Stams, Jessica J. Asscher, Mark Assink. "Risk factors for juvenile cybercrime: A meta-analytic review. Aggression and Violent Behavior". Volume 70, 101836. May–June 2023. <https://doi.org/10.1016/j.avb.2023.101836>
- [6] Zabarniy, Maksym; Topchii, Vasyli; Korniakova, Tatiana; Topchii, Oksana; Topchii, Vitalii. "Criminological Analysis of Determinants of Criminal behavior". Journal of Forensic Science and Medicine 9(2);p 144-152. Apr–Jun 2023. DOI: 10.4103/jfsm.jfsm\_84\_22
- [7] Richelle Mayshak, Dominika Howard, Michelle Benstead, Anna Klas, David Skvarc, Travis Harries, Brittany Patafio, Abby Sleep, Ross King, Shannon Hyder. "Dating in the dark: A qualitative examination of dating experiences in Dark Tetrad personalities School of Psychology". Deakin University, 1 Gheringhap Street, Geelong, VIC, 3220, Australia. Computers in Human Behavior Volume 143. June 2023. <https://doi.org/10.1016/j.chb.2023.107680>
- [8] European Union Agency for Criminal Justice Cooperation (Eurojust). 2002. [Online]. Available: <https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/cybercrime> [Accessed: March 24, 2024].

# Gamma-background radiation control systems as a factor of Bulgaria's national security

**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:  
Dolna Mitropolia  
nicheff@abv.bg

**Abstract.** The sources of ionizing radiation and nuclear facilities on the territory of Bulgaria may cause a change in the radiation gamma background in the event of an accident or accident. With the conduct of military operations on the territory of Ukraine and in the Middle East, this danger should not be underestimated.

Already in the 90s of the last centuries, systems for monitoring the radiation background were being built in Bulgaria for various ministries and departments. The report reviews some of these systems, analyzes their positive and negative sides, and makes recommendations for improving their functioning and optimizing the submitted data.

**Keywords:** automated system, gamma radiation background, monitoring station, radiation, national security, probe characteristics, values.

## I. INTRODUCTION

After the major accident at the Chernobyl nuclear power plant, located on the territory of the current Ukraine, and then in the USSR, in April 1986, in Bulgaria, as well as in most European countries, the lack of systems for continuous measurement of the radiation gamma background was reported, to provide reliable information in real time about the radiation status [1], [2], [3], [4]. In the second half of the twentieth century, the use of sources of ionizing radiation expanded significantly - nuclear power plants were built, medical diagnostics expanded, and radiation using these rays also entered industry. But the Chernobyl accident became a prerequisite for monitoring the use of ionizing radiation and controlling environmental pollution with such radiation. As a result, in the countries of Europe and around the world, the construction of automated systems for continuous monitoring of the gamma-background radiation and their integration into national security and their connection in various international networks have begun [5], [6].

In Bulgaria, the construction of the National Automated System for Continuous Control of the

Radiation Range - background in the Republic of Bulgaria (BULRaMo) also began in 1992 by the German company "Hormann" - GmbH. In 1997, it was put into operation in accordance with the Ordinance on the Construction, Operation and Development of the National Automated System for Continuous Control of the Radiation Gamma Background in the Republic of Bulgaria - PMS No. 434/19.11.1997. The department responsible for building and maintaining the system is the Ministry of Environment and Water (MOEW) through the Environmental Executive Agency (EAOS), with financial resources under the PHARE program [7], [8]. The built control system covers the territory of Bulgaria and is the only national network. There are such systems built for other ministries and departments, but they are not intended for use by the entire population and have to solve specific tasks - there are such systems built for the Ministry of Defense, the Ministry of Internal Affairs, the former already Civil Defense and others.

## II. MATERIALS AND METHODS

The main purpose of this national real-time radiation control system is:

- Continuous monitoring and monitoring of the gamma-background radiation level on the territory of the entire country and the storage of the obtained information in a national database, with the monitoring points selected based on the availability of such objects, the availability of resources, population density and others.

- Early disclosure in the event of an increase in the level of gamma-background radiation as a result of an accident of a different category with radiation pollution of the environment or a conflict with the use of nuclear weapons on the territory of Bulgaria or in its vicinity.

- Submission of operational information to the relevant state bodies responsible for the radiation situation in Bulgaria and making the relevant decisions.

- Submission of operational information to the European Radiological Data Exchange System

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8225>

© 2024 Nikolay Todorov Dolchinkov, Nikolay Bonev Nichev.

Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

(EURDEP), the Agency for the Use of Nuclear Energy for Peaceful Purposes (IAEA) and other organizations with which Bulgaria has data exchange [9].

In 1997, the work of the National Automated System for Continuous Gamma-Background Radiation Monitoring (BULRAMO) under the Ministry of Environment and Water began.

In 1999, all Local Monitoring Stations (LMS) on the territory of Bulgaria were finally launched and included in the system for autonomous operation in online mode.

In 1999, the Automated Information System for External Radiation Control of the Kozloduy NPP was integrated into BULRAMO, which expanded the range of radiation gamma-background monitoring with another 8 LMS in the area of the Kozloduy NPP, where two power units operate of the water-water energy reactor type VVER-1000 [10].

In the same year, the Central Station (CS) software was successfully upgraded to run under Microsoft Windows 2000 Server and Microsoft SQL 2000 Server, due to their better qualities than the previous operating system [1], [10].

After the expiration of the warranty service in 2001, the post-warranty service of BULRAMO started, as the company "PROSERVIS NT" Ltd. has built a service base for the repair of practically all components of BULRAMO.

The BULRAMO system was integrated into the European platform for the exchange of radiological data - EURDEP in 2003. As a member country of EURDEP, Bulgaria is obliged to send a continuous flow of data on the state of the radiation background, as well as has the right to real-time access to information from similar systems of the EU member states. Bulgaria's access to EURDEP is extremely important in the event of a nuclear accident or nuclear conflict and is carried out online [11].

In 2004, the IAEA started issuing a daily bulletin about the radiation situation in the country on its website every day without Saturdays, Sundays and holidays, which is visible to all users.

In 2005, the Ministry of Defense, through the Centre for Collection, Processing and Analysis of Information on Nuclear, Chemical and Biological Situations, became a user of BULRAMO's operational information, and an Additional Monitoring Centre was built on its territory.

The same year, the Ministry of Health, through the National Medical Coordination Centre, became a user of BULRAMO's operational information, but did not build an Additional Monitoring Centre, unlike the Ministry of Défense.

In 2008, the State Enterprise "Radioactive Waste" (DP "RAO") built a Local Monitoring Station for continuous control of the radiation gamma-background in the municipality of the village of Novi Khan, due to the increased public interest in the level of radioactivity, around the existing repository for radioactive waste - Novi Inn. This is currently the only repository for radioactive waste on the territory of the Republic of Bulgaria. The newly built station is technically fully compatible with the

Central Station of BULRAMO and through its integration, the system has been expanded with a new station owned by DP "RAO". The new repository for radioactive waste, which will be located adjacent to the Kozloduy NPP, falls within the range of the plant's local monitoring stations.

After the Fukushima accident in 2011, the BULRAMO system switched from daily to hourly reporting to the European Radiological Data Exchange Platform - EURDEP. This was dictated by the need to monitor the radioactive background and increase the security of the population and the state.

Later in 2013, the IAEA started issuing the daily bulletin on the radiation situation in the country and on weekends, all done automatically.

In 2013-2014, the BULRAMO system was updated according to the project of the operational program "Environment 2007-2013". All measurement sensors, communication channels, computer equipment and the specialized software serving BULRAMO have been updated. An additional 16 spectrometric gamma probes have been installed [12], [13].

In addition to the daily bulletin, the EAOS page now provides information on the last 24 hours in real time through the EURDEP widget from BULRAMO and the systems of other European countries. At the same time, the information is updated every 10 minutes on working days and every 30 minutes on weekends and holidays. If necessary, these renewal intervals can be made smaller if the security of the population requires it [4].

### III. RESULTS AND DISCUSSION

#### Structure and equipment of BULRAMO at launch and operation in 1997.

1. BULRAMO consists of:

- 26 Local Monitoring Stations (LMS) equipped with:
  - o Gamma probe: IGS421B.
  - o Rain detector: RD200
  - o Computer data logger (Data logger) – DLM1440
  - o Communication equipment – mast with antenna
  - o Meteorological stations in 8 of the LMS: AMC100.
- Radio channels for transmitting the measured values.
  - o Repeater stations.
  - o Radio communication centers (RCCs).
  - o Central station (CS) located in the building of the Environmental Executive Agency (EAOS) carrying out:
    - o Communication and transfer of LMS data.
    - o Storage of the received information in a database.
    - o Visualization of the radiation and technical status of the LMS.
      - o Generate newsletters from the database.
      - o Data replication to the Additional Monitoring Centres.
        - o Alarm notification in case of increased values of radiation gamma-background.
  - Additional monitoring centres (DMCs), performing monitoring and analysis of the data replicated by the CS.
  - Mobile monitoring station – A vehicle equipped with the equipment of an LMS.
  - In addition to BULRAMO are joined:

o 8 LMS from the Kozloduy NPP external radiation control system. These stations are under the administrative and technical management of Kozloduy NPP. Data from these stations is received via radio channel and stored in the BULRAMO database.

o 1 LMS of DP "RAO" - town of Novi Khan. This station is under the administrative and technical management of DP "RAO". Data from this station is received via radio channel and stored in the BULRAMO database.

The location of the local monitoring stations on the territory of Bulgaria is shown in figure 1.

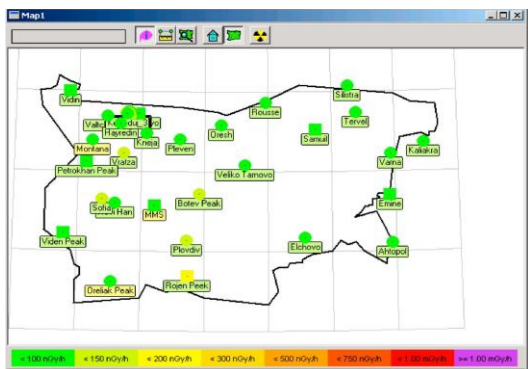


Figure 1: LMS location on the map of Bulgaria - view from the old visualization program (label color - technical status, station color - radiation status)

## 2. Data stored by BULRAMO:

- 10 minute average value of absorbed dose rate (air kerma) in units of nGy/h generated by IGS421B.
- Presence or absence of rain.
- Technical status for IGS421B.
- Technical status for DLM1440.
- CS calculates hourly and daily averaged values for absorbed dose power based on 10-minute averaged values.

## 3. Structure and equipment of BULRAMO after the renewal of the automated system.

The BULRAMO system was updated according to the project of the operational program "Environment 2007-2013" in 2013-2014 [14].

The reason for the update is that at the time the update started, a number of components were out of date. Additionally, from the start of the system's operation in 1997 to 2013, there have been significant developments in computer and communication technology, making old equipment technically incompatible with new computer and communication components. It is necessary to replace many of the gamma probes because they are morally obsolete and their defects are becoming more frequent [3], [15]. The overall architecture of BULRAMO has been assessed as successful and has been preserved. The renewal of the National Automated System for Continuous Control of the Radiation Gamma Background – BULRAMO covers:

- LMS
- Communication channels
- The central station
- The mobile monitoring station
- The additional monitoring centres

## 4. Local monitoring stations.

All measuring sensors have been renewed, additionally installed in 16 of 26 LMS spectrometric gamma probes. The manufacturer of the gamma probes and rain detectors is ENVINET GmbH. The new installed components are:

- Gamma probe: IGS421B -H measuring power of the ambient equivalent dose in  $\mu\text{Sv}/\text{h}$ .
- Rain detector: RD203.
- Computer data logger (Data logger) – DLM1440 has an improved ARM based processor module with embedded Linux and Lan interface.
- Spectrometric gamma probe – SARA IGS 710/910 (NaI/LaBr<sub>3</sub>).
- Communication equipment – GPRS/3G and the communication equipment of the radio channels is preserved.
- Meteorological stations – IAES has no obligation to measure meteorological parameters, and due to the fact that the main manufacturers of equipment for radiological monitoring systems in the environment do not offer such equipment, the available weather stations are preserved but their renewal is not foreseen.

## 5. Communication channels.

An IP/VPN network of GPRS/3G modems in LMS and DSL modems in CS and some DMCs was built, which became the main communication environment. Radio channels are preserved as backup communication channels, but due to their low transfer rate they cannot transfer the data to the gamma spectrometer probes. The new communication environment (GPRS/3G) allows the communication sessions from an interval of 30 minutes for the radio channels to go to an interval of 10 minutes, using optical wires for this purpose [5], [16].

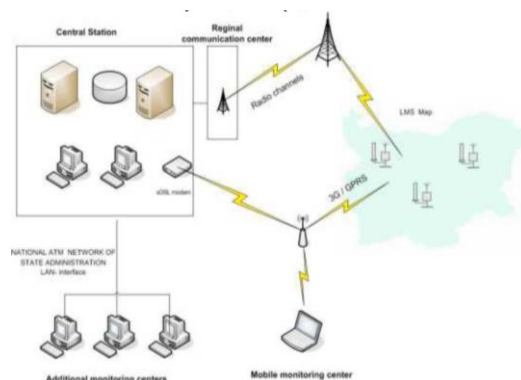


Figure 2: Schematic of the updated BULRAMO communication environment

## 6. The central station.

□ The CS software equipment was based on Microsoft Windows Server 2012, Microsoft SQL Server 2012 and a specialized software package countries ts.Net developed specifically for the renewal of BULRAMO. The countries ts.Net package includes modules for:

- Communication and data transfer from LMS.
- Storage of the received information in a database.
- Visualization of the radiation and technical status of the LMS.
- Generate newsletters from the database.

- Data replication to the Additional Monitoring Centers.
- Alarm notification in case of increased values of radiation gamma-background.
- The servers and workstations serving BULRAMO's CS have been replaced.

#### 7. The additional monitoring centers.

The software equipment of DMC is based on Microsoft Windows 7, Microsoft SQL Server 2012 express and specialized software package countries ts.Net. At a later stage at the beginning of the third decade of this century, a higher level of operating system was already used. Table captions and titles should always be right aligned and placed above the tables. Tables are numbered consecutively with Roman numerals and have reference in the main text [6], [17], [18].



Figure 3: Mast of LMS Rozhen - Gamma probe and Meteo station

Figures 3 and 4 show pictures from the LMS operating in the NASNKRGF and a comparison between the old and new probes.



Figure 4: Photo of the upgraded sensors on an LMS. On the left is the spectrometry probe, in the middle is the start and on the right is the new dosimetry probe

Also of interest are the radioactive contamination control systems at the NIMH, where a radioactive contamination prediction system operates in the event of an accident in some of the nuclear power plants located on the European continent [1], [2], [3], [19]. A disadvantage of this system is that too few people know about it and it is more unrecognizable to the population.

The BERS (Bulgarian Emergency Response System) system works operationally every day at NIMH, calculating trajectories, concentrations and depositions (deposits on the earth's surface). The WRF meso-meteorological model is used, which is fed with prognostic information from the American GFS (Global Forecast System) with a resolution of 0.25 deg and makes a forecast three days ahead for the area of Europe. Wind information in space and time is used in the calculation of forecast trajectories. Concentrations and depositions are calculated from the three-dimensional model EMAP (Eulerian Model for Air Pollution) created at NIMH for describing the distribution of atmospheric pollutants. The meteorological input of the model is the WRF-calculated prognostic fields of a number of meteorological parameters that determine the intensity not only of transport, but also of a number of other dispersion processes such as diffusion, dry and wet deposition, chemical and radioactive transformations, etc. As a source of pollution, a simulation of a powerful nuclear accident was used, the parameters of which are described on the right of the animated picture [6], [20].

Visualized maps are a forecast, not a real situation. In them, the eventual spread of radioactive contamination within 72 hours after the occurrence of the accident is done on an hourly basis and the development of the process over time is visualized. The results are achieved on the basis of the forecast of the speed and direction of the winds in the area of the accident at different altitudes. The selected elevations are 100, 300 and 1000 meters above the surface of the Earth's crust in the area.

The BERS (Bulgarian Emergency Response System) system works operationally every day at NIMH, calculating trajectories, concentrations and depositions (deposits on the earth's surface). The WRF meso-meteorological model is used, which is fed with prognostic information from the American GFS (Global Forecast System) with a resolution of 0.25 deg and makes a forecast three days ahead for the area of Europe. Wind information in space and time is used in the calculation of forecast trajectories. Concentrations and depositions are calculated from the three-dimensional model EMAP (Eulerian Model for Air Pollution) created at NIMH for describing the distribution of atmospheric pollutants. The meteorological input of the model is the WRF-calculated prognostic fields of a number of meteorological parameters that determine the intensity not only of transport, but also of a number of other dispersion processes such as diffusion, dry and wet deposition, chemical and radioactive transformations, etc. As a source of contamination, a simulation of a powerful nuclear accident was used, the parameters of which are described on the right of the animated picture [4], [5], [8].

Two types of information are presented on a BERS system page:

Predictive trajectories of particles released at different altitudes over selected 36 European nuclear power plants. In their calculation, only the three-dimensional wind field was taken into account. In other words, only one of the many dispersion processes - transport - is modeled.

The animated prognostic fields of concentrations and depositions of radioactive material discharged from each

of the above plants, taking into account not only transport, but also other dispersion processes: diffusion, dry and wet deposition on the earth's surface, transformation of pollutants, etc.

Initially 49 NPPs were selected in the system, but at a later stage they were reduced to 36.

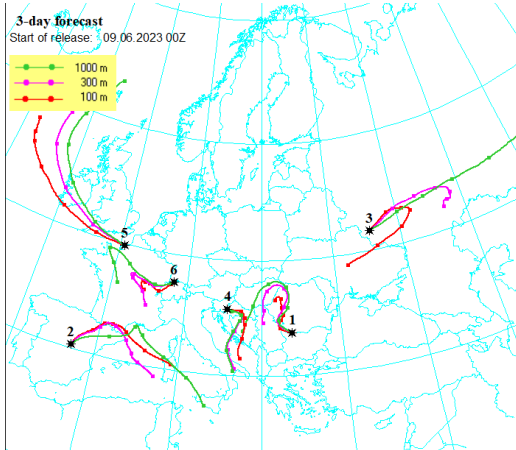


Figure 5- Forecast of radioactive contamination

In fig. 5 shows the results for the possible spread of radioactive contamination at a height of 100, 300 and 1000 meters above the ground level after 12, 24, 36, 48, 60 and 72 hours after an accident at 6 NPP - 1 - Kozloduy, Bulgaria, 2 - Jose Cabrera, Spain, 3 – Kursk, Russia, 4 – Krisno, Slovenia, 5 – Papuel, France and 6 – Leibstadt, Switzerland. Analogous maps can be seen for the other NPPs that the system monitors and forecasts.

In fig. 6 shows a similar map of pollution as a result of a possible accident, and here under No. 20 is the Zaporizhzhia NPP, which is on the territory of Ukraine and is under the control of Russian forces and the monitoring of the IAEA. It is of interest to us because it is located close to us, the predominant part of the winds would bring radioactive pollution to Bulgaria, and military operations are taking place near it.

A visualization of 3-day forecast trajectories of particles released from selected nuclear power plants in Europe can be called up by clicking on the tabs above the image. The 36 NPPs are presented in groups of 6 for better visibility. The names of each NPP can be found by number from the list on the right.

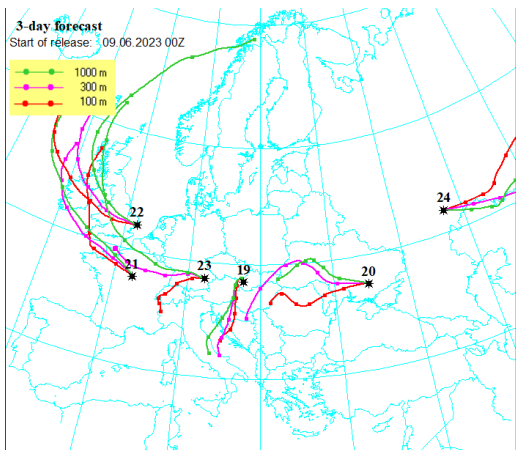


Fig. 6. Forecast of radioactive contamination

The depicted trajectories from each point correspond to 3 release heights: 100 m, 300 m and 1000 m

The start time of each trajectory is 00:00 of the current day. The points on each trajectory determine the position of the particle after 12, 24, 36..., 72 hours. The positions of the NPPs themselves are shown with asterisks.

Concentration and deposits (menu on the right)

Hovering over a NPP name in the list on the right brings up a drop-down menu with 2 options: Concentration and Deposition, which are links to animations of a simulated nuclear accident. The parameters of the accident are fixed (shown in the animation) and simulate a powerful release of radioactive material.

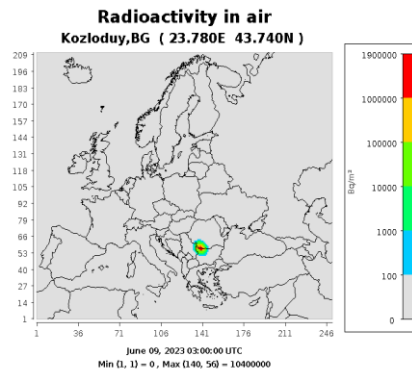


Fig. 7. Concentration of pollution during an accident at the Kozloduy NPP

In fig. 7 shows the concentration of pollution in the event of an accident at the Kozloduy NPP, and in fig. 8 shows the concentration of deposits on the soil during an accident at the Zaporozhye NPP. A snapshot of the two animations was taken, but the site itself tracks the dynamics of changes in the concentration of radioactive air pollution and radioactive deposits on the soil. Forecasts are made on the basis of the current movement of air masses and the forecast for its change within up to 72 hours after the accident.

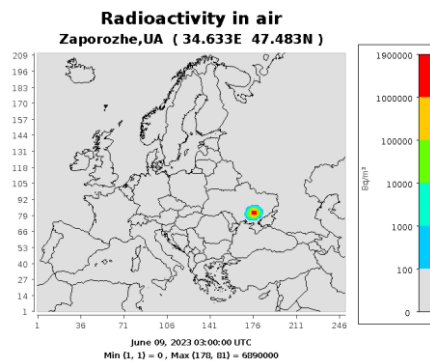


Fig. 8. Concentration of deposits during an accident at the Zaporizhzhia NPP, Ukraine

Due to the nature of the other radioactive control systems, their operation is not analyzed in this article. They have specific purposes and serve a specific category of users and are mainly used for business purposes.

#### IV. CONCLUSIONS

1. The National automated system for continuous control of the radiation range is well developed and organized - background in the Republic of Bulgaria for informing the population in case of radiation incidents;

2. The radiation gamma background is within the limits of background values typical for the country and in recent decades there have been no deviations from the normal values for the specific regions. The values of each station are different because the natural radioactive background is not the same;

3. A program for ensuring nuclear safety has been developed and is being implemented, but a consistent and predictable policy of the authorities in the field of the use of sources of ionizing radiation, including power units, is needed. Bulgaria lacks consistency and transition between governments regarding the development of nuclear energy and its safety. There is decision making with political advantage but without broad professional expertise.

#### 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 p. 1;
- [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 p. 27;
- [4] Communication from the commission to the council and the european parliament. Communication on nuclear non-proliferation, Brussels, 26.3.2009;
- [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): p.38-44
- [6] S. Vambol, V. Vambol, V. Sobyna, V. Koloskov, L. Poberezhna, Investigation of the energy efficiency of waste utilization technology, with considering the use of low-temperature separation of the resulting gas mixtures, ENERGETIKA. 2018. T. 64. Nr. 4. P. 186–195, © Lietuvos mokslų akademija, 2019
- [7] N.Dolchinkov and N. Nichev, Structure and Management of the National Automated System for Permanent Control of the Radiation Gamma Background in Bulgaria, De gryuter open, Land Forces Academy Review Vol. XXII, No 2(86), 2017, Sibiu, Romania, p 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 p. 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.P. Stefanova, V.P. Vasilev, I.P., Efreimovski, 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; <https://www.igi-global.com/gateway/chapter/325452#pnlRecommendationForm>
- [12] D.N.Todorov, 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, p 7-18. Available: <https://www.researchgate.net/publication/321905753>
- [14] 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
- [15] N.Dolchinkov, Optimization of the systems for monitoring and public disclosure of radioactive contamination of the environment, International journal „Knowledge“, Skopje ISSN 1857-92 Vol 15.1 p. 423-431 GIF 1.023 (2015) . Available: <https://www.researchgate.net/publication/320378173>
- [16] N.Dolchinkov, Analysis and Optimization of the National Automated System for Continuous Control of the Radiation Gamma Background, Third National Congress of Physical Sciences, Sofia, September 2016. ISBN 978-954-580-364-2 Available: <https://www.researchgate.net/publication/313109065>
- [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, pp: 235, 2016
- [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. 84-9
- [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



# *Hazards posed by the war in Ukraine: A study of population information risk and mitigation efforts*

**line 1: Petko Dimov**

line 2: *Department of Distance  
Learning, Language Training and  
Qualifications*

line 3: *Rakovski National Defence  
College*

line 4: Sofia, Bulgaria

line 5: p.dimov@rncd.bg

**line 1: Georgi Marinov**

line 2: *Department of Logistics*

line 3: *Rakovski National Defence  
College*

line 4: Sofia, Bulgaria

line 5: g.marinov@rncd.bg

**Abstract.** The Russian-Ukrainian conflict is the most significant security crisis since World War II. Intense fighting has irreparable effects on water, air, soil, and the ecosystem. They are leading to a massive loss of life and unfolding social and humanitarian disaster in the Black Sea region.

Even more significant, however, is the information disaster in cyberspace, which has gone far beyond these borders and even affected the whole world.

This study reviews available normative documents to examine the maximum amount of documents related to managing Russia's and Ukraine's combat operations in information warfare.

Access to the state electronic databases of Russia and Ukraine, which provide access to many normative documents, was used to fulfill the set objective. These are the "Official web portal of the Parliament of Ukraine" (Verkhovna Rada of Ukraine) and "The Federal Assembly" of the Russian Federation (The State Duma).

The aggregate number of sources examined is 83564. Based on the criteria for inclusion, the total number of articles analyzed was reduced to 216, as they specifically pertain to security in information and cyberspace.

The research findings on information risk between the two countries indicate that their primary focus was ensuring cyber security following the outbreak of war. However, one of the initial priorities was to address the safeguarding of e-government and the information security of citizens. Subsequently, steps were implemented to combat false information and coordinate their media, which was crucial to the operation's success.

The analysis indicates that Russia is presently experiencing defeat in the information war between the Western world and Ukraine. However, it is achieving resounding success within its borders and is garnering support from Chinese citizens as well as other isolated nations like Iran and North Korea. Partial achievements have been observed in Asia and Africa. However, the situation could rapidly shift due to the superior influence of

Western powers on popular social platforms, including Facebook, Twitter, Instagram, YouTube, and Google.

This conflict has transcended into more than a mere battle between two nations and their military forces. It embodies the form of an impending conflict—the war behind the war.

**Keywords:** *cyber operations, cyberwar, information operations, warfare*

## I. INTRODUCTION

The war between Russia and Ukraine is the most significant security crisis since World War II. Intense combat is causing irreversible damage to water, air, soil, and the biosphere, resulting in substantial casualties and a developing crisis in the Black Sea region. This poses specific political, economic, and energy dangers for Europe. The information catastrophe in cyberspace has extended beyond boundaries and impacted the entire planet.

The article analyzes normative activity and legal actions in the information sphere and cyberspace. It examines 83564 normative documents issued by the Russian Federation and Ukrainian governments during the war, as published in state electronic databases.

## II. METHODOLOGY

This study reviews available normative documents to examine the maximum amount of documents related to managing Russia's and Ukraine's combat operations in information warfare.

Access to the state electronic databases of Russia and Ukraine, which provide access to many normative documents, was used to fulfill the set objective. These are the "Official web portal of the Parliament of Ukraine" (Verkhovna Rada of Ukraine) and "The Federal Assembly" of the Russian Federation (The State Duma).

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8229>

© 2024 Petko Dimov, Georgi Marinov. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

The search principle for articles used the following keywords: 'Information operations' AND 'cyber operations'; 'cyberwar' AND 'information warfare\*'; 'Ukraine' AND 'Russia'; 'cybersecurity' AND 'information security'.

As the topic is relatively new, a limit of documents was set for the period 14 May 2021 until 3 January 2024.

Inclusion criteria

- 1.) Official documents are published in English or Russian.
- 2.) Normative documents related to changes in information and cyber security
- 3.) Official normative documents issued by Ukraine and the Russian Federation governments.
- 4.) Influence on own, opposite, and allied citizens.
- 5.) Unclassified documents issued by Ukraine and the Russian Federation were used.

### III. RESULTS AND DISCUSSION

#### *Ukraine's Actions in the Information Domain.*

The normative activity of Ukraine after the start of operations was studied, and 45151 legal decisions and decrees were reviewed from the web portal of the State Rada (zakon.rada.gov.ua), 142 of which affect the population in the domain of information.

Strategic Communications Strategy, Information Security Protection Strategy, and Cybersecurity Strategy [1] were adopted before the start of the war and updated promptly just before the war by Decree No. 447 of 14 May 2021.

The "Basic Principles of Cyber Security Act" also governs changes by wartime laws, for example. It defines the objects of critical information infrastructure and the requirements for the various actors.

In other words, it can be said that Ukraine has a relatively modern legal framework in the field of cybersecurity. In the field of information security, changes are required with the entry into force of the "Presidential Decree on Martial Law", such as, for example, the early graduation of cadets from the Institute of Special Communication and Information Protection of the Polytechnic University of Kyiv [2].

To counter the massive cyberattacks at the start of the 08 March war, Decree 42 ordered banks and government organizations to store their users' data in cloud storage only in the EU, the United Kingdom, the United States, or Canada [3]. In this connection, a law was passed on 13 March to ensure the functioning of information and communication systems and public electronic registers, stipulating that backup copies be created for storage outside the occupied territories. On 15 March, the Criminal Procedure Code was updated to counter cyberattacks. The Law on Electronic Communications was adopted, changing the "Procedure for maintaining a register of providers of electronic communications networks and services" and the means for their certification.

One of the first things that the Ministry of Digital Transformation of Ukraine is doing is to create an electronic identity document during the martial law period (eDocument), which provides information about the

person using the mobile application Diia, and this is done automatically, without the presence of the user through the "Unified state web portal for electronic services".

On 19 March, Decree 151 was issued to neutralize threats to the country's information security, with digital terrestrial radio and television facilities operating around the clock from a particular wartime location. Taking into account the direct military aggression of the Russian Federation, the active dissemination of disinformation by the aggressor state, the distortion of information, as well as the justification or denial of the armed aggression of the Russian Federation, Decree No. 152/2022 of 19 March 2022 of the President of Ukraine on the implementation of a unified information policy under the law of war is issued. A unified information policy is a priority issue of national security, which is implemented by combining all national TV channels, whose program content consists mainly of information and analytical programs on a unified information platform for strategic communication "United News #UArazom".

All activities about the collection, processing, and dissemination of official information products shall be assigned to the Ukrainian National News Agency "Ukrinform", and the production and broadcasting of television and radio programs to the State Enterprise "Multimedia Platform for International Broadcasting of Ukraine", the latter being allocated additional funds for the creation of a Russian-language television project "Svoboda". Two programs are also established: the "Development and Modernization of the State Special Communication and Information Protection System" and the "National Information Program" to ensure the protection and uninterrupted operation of the National Telecommunications Network and critical information infrastructure facilities - national electronic information resources and state information and communication systems.

A law banning the propaganda of the Russian neo-Nazi totalitarian regime, and the symbols used by the armed and other military formations of the Russian Federation in the war against Ukraine, has been adopted.

Already in the early days of the conflict, Ukraine broadcast many products that evoked strong emotions to boost the patriotism and morale of its audience. Messages are broadcast on all channels, focusing on the internet and social media. All announcements are initially approved and published in official channels or online conferences and subsequently distributed in social groups, Facebook, Twitter, YouTube, etc [4]. Telegram was not left out, so several groups and applications were created.

Ukraine's online propaganda primarily focuses on its heroes and martyrs who tell the story of Ukrainian courage. This is a classic example of modern propaganda that is critical to the narrative that Ukrainians are fighting for a just cause and will win this war. These messages must influence the hearts and minds of their citizens. This is especially important in this conflict as the Ukrainians try to maintain high morale among their fighters.

Modern means include cyberattacks, viral messaging, and drowning the opposing narrative in a sea of adversary content. This is why new wars are developing at breakneck speed on social media and official websites, and more

content is needed to spread the messages of our narrative and drown out that of the enemy. Social media has become a significant channel for pushing information, and tech companies can play a role in the information war, whether they are vetted or not.

Ukraine's strategy for influencing an allied audience relies on creating emotions that evoke patriotism and support. Constantly broadcast clips of the President of Ukraine created a patriotic, courageous image of Volodymyr Zelenskyy, who presented himself as a hero seeking support.

This is why the Ukrainian government turned to Western social media, showing an excellent understanding of information technology and modern marketing techniques. For example, the "Hero Stickers" initiative was created on Twitter to bring together various hacking organizations to carry out cyberattacks against Russia with remarkable results. The world's largest hacking organization, Anonymous, attacked Russian government websites, including access to personal data stored on the Ministry of Defense of the Russian Federation website. According to Chinese sources, 27% of DDoS attacks on Russian sites were launched in the US, which is unlikely to have been carried out by individual hackers but rather the work of an organized government force [5].

In the fight for the enemy audience, the Armed Forces of Ukraine started to search for contacts on social networks of relatives of captured and killed Russian soldiers and tried to communicate with them in an attempt to create mass discontent against the government. One striking example in this area is the website "The Project", which identifies the names of Russian commanders of troops and units taking part in a particular operation. "Project" publishes a database with information about the Russian army units involved in the war, which area of the country they came from, and the names of their commanders. A particular unit of hackers investigates the biographies of these officers and the state of the military units they command, tracks down their relatives, and attempts to influence them on social networks.

Investigations that fuel stereotypes about Russians have also been published. According to the state website, "the average income of division commanders in 2019 was 160 thousand rubles (2348 euros at the current exchange rate). They also own a small apartment, with 1/3 of the officers having mortgage loans, and 1/4 having traffic tickets, some for drinking". But we must remember that they should be looking for bad examples, scandals, corruption, and other misdeeds to publicize.

After the rapid update of the legislation at the beginning of the war, Ukraine already had modern legislation in the field, but it did not stop there. It continued to adapt to enemy actions and to propose new initiatives in the information domain. The Ministry of Defence has launched a new digital service app that reduces the administrative burden on soldiers in combat. On April 24, 2023, the Restart in Cyberspace project began training citizens ages 25 to 60 to help in the field. At the end of 2023, the adopted Action Plan for 2023-2024 for implementing the Cybersecurity Strategy of Ukraine was published. It states that for the first quarter of 2024, the

Ministry of Defense should establish a cyber military in the MoD system and a military incident response center. It was establishing a national cyber-attack detection system, countering acts of cyber-terrorism, and establishing a cyber-intelligence system [6]. Improve regulatory, organizational, and personnel support for the national system, and improve training of employees, etc.

#### *Actions of the Russian Federation in the Information Domain.*

In the government website publication.pravo.gov.ru, a search for regulatory documents signed in the period 24 February 2022 to 3 January 2024 found 38413 results of the Russian Duma, the Government, and decrees of the President of the Russian Federation, of which almost 74 concerned security in information and cyberspace.

The documents show that in an attempt to protect its audience, Russia is also stepping up efforts to block, restrict, and control the various foreign social platforms and providers operating on its territory. The Presidential Decree prohibits using foreign security at critical information infrastructure sites [7].

As soon as the war began, Deputy Prime Minister Dmitry Chernyshenko instructed the Russian Ministry of Digital Development, Communications, and Mass Media to prepare priority measures to protect the country's information infrastructure. As a result, measures taken include allocating funds to support the IT industry, increasing salaries for employees in the IT sector, granting support for promising local IT solutions, and providing preferential loans to IT companies for ongoing operations and implementation of new projects.

Yandex, Rostelecom, and VK immediately announced that they would provide their public "clouds" to maximize the speed of state sites. According to a leaked government telegram published on Nexta, the Deputy Prime Minister has ordered all government websites and web services to switch to Russia's ".ru" domain name system by March 11 and to switch to using DNS servers located on Russian territory, as well as to "complicate the password policy" [8].

In addition to stopping foreign hosting, a decree is issued with additional measures that stop traffic counters, analytics tools, and banner ads provided by foreign companies, such as Google Analytics [9].

Already on the ninth day of the war, the State Duma passed a law on punishment for spreading fake news related to the actions of the Russian armed forces, which imposes a fine of 700,000 to 1.5 million rubles or up to 3 years in prison. If this has led to severe consequences - from 10 to 15 years in prison [10], i.e., anyone can not spread whatever information they want about the events in Ukraine. Still, only such information originates from official Russian institutions. That is why most websites and blogs are silent on this issue, lest they make a mistake somewhere and get fined or imprisoned [11].

At the beginning of the third week of the war, the Prosecutor General's Office of the Russian Federation asked the court to recognize the technology company Meta as an extremist organization and ban their activities in Russia based on Article 280 and Article 205.1 of the

Criminal Code of the Russian Federation for “public calls” to carry out extremist activities and promote terrorist activities on Facebook and Instagram, and for having discriminated against state media since 2020. With this decision, the government blocked Facebook and Instagram and then suggested that government agencies create accounts on domestic social networks such as RuTube (for video), VK (a Facebook clone), Fiesta (like Instagram), and Telegram. Gazprom Media, too, created a kind of TikTok called Yappy.

Google and YouTube stopped selling online ads in Russia, and TikTok stopped live streaming and publishing new content in the country [12]. Twitter has announced that some users in Russia cannot access the social network. Microsoft banned sales to Russian citizens following a similar move by Apple. BBC, Voice of America, Deutsche Welle, and Radio Free Europe were blocked. The independent Echo of Moscow radio was taken off air for continuing to call what was happening in Ukraine a “war”. The same was the fate of the opposition television “Dozhd”.

These actions will likely make it difficult for most Russian citizens to see an adversary’s point of view. Still, a recent Levada Center survey shows that nearly a quarter of Russian citizens surveyed use VPNs to access blocked websites, citing connection points outside Russia [13].

The restriction on access to foreign technologies and communication platforms forces users to rely on alternative and available services from Russian companies, and the Russian authorities strictly control these services.

Since the start of the war in Ukraine, Russian users have had significant problems accessing government websites and online banking clients.

Several dozen organizations in the world have digital master certificates, but 75% of them are issued by just five of the largest companies that are based in the US [14].

For this reason, the Ministry of Digital Development, Communications and Mass Media of the Russian Federation offers its master certificate from which subsidiary public service certificates are issued. The problem is that browsers like Chrome, Safari, Microsoft Edge, and Mozilla don’t recognize this certificate. Therefore, Russian users must manually add the Russian certificate to the trusted list or switch to Yandex and Atom’s Russian browsers. Since the certificate is state property, installing it is trusting the authorities.

Regarding the enemy audience, the Russians’ strategy combines physical influence, cyberattacks, information, and psychological operations conducted by previously prepared powerful formations.

Among the first targets in the military operation were critical elements of Ukraine’s media and communications infrastructure. Proof of this is the first object destroyed by sabotage – the main television repeater in Eastern Ukraine. Subsequently, mobile operators’ base stations have been impacted by sabotage and fire strikes, hacking attacks for data theft, DDoS of important portals and official websites with botnets of the “Maray” type, and signal jamming by radio electronic warfare units [15]. Because of this, there are almost no Ukrainian mobile operators in Crimea and

Eastern Ukraine and no Ukrainian radio and television stations.

In cyberspace, information is initially gathered through phishing, the purchase of compromised data from hacker forums, and attacks to access address books of mail servers. Typical social engineering techniques or direct penetration through software vulnerabilities in management systems are used for penetration. Next is the internal distribution of the malicious “NotPetya” type code and the theft of data and its transmission via encrypted communication software such as the Telegram Group API or the theft of files using Robocopy, which copies them to an additional cloud drive.

In the adversary’s information space, the Kremlin, through direct or indirect funding, creates disinformation content, maintains “factories” of trolls, and distributes this content in a coordinated manner on social networks. These “trolls” are most often people working from home who create and maintain fake (and, more recently, real) profiles, which they use on command to share “news” in groups and pages, as well as writing comments under news articles [16]. This, in turn, leads to algorithmic amplification of these posts (because lots of people are interested), with Facebook (and other social networks) showing it to more and more people.

Regarding the strategy of influencing the allied audience, what often fails to be understood is that Russian propaganda, despite popular belief, is not mainly focused on the Western world. Russia is aware that, for the most part, the people here are hostile to Russia, and nothing will change that. However, gaining popularity in Africa and Asia is an achievable goal and is undoubtedly the focus of Russian information and psychological operations. For example, we might see a news story about a difference in behavior toward Ukrainian and black refugees that does not impact us but has a significant impact in India or Africa [17]. While this news has no repercussions in Europe, countries like Nigeria may have a different view [18].

Russian propaganda pays special attention to China, even though all the fighting events are accompanied by live reports from Chinese journalists, stating that the Chinese do not support NATO enlargement [19]. The Carter Center China Focus provided the first poll of Chinese public opinion on Russia’s invasion of Ukraine in April. The results show that 75% of respondents agree that supporting Russia in Ukraine is China’s national interest [20]. However, more than 60% of respondents support a neutral policy through moral support without supplying arms to Russia. Notably, only 16% of respondents support providing arms to Russia, only 3% more than those who believe China should change its current course and condemn the Russian invasion. Moreover, the Chinese Foreign Ministry spokesman also repeatedly blames NATO for getting too close to Russia’s borders.

Television crews with pre-prepared reports or cameras positioned to film the enemy for provocation are widely used in information warfare. For this purpose, formations are deployed and fire from kindergartens, schools and residential or public buildings. Within 1 - 2 hours after the event, reports are broadcast in which actors play. Russian television and news agencies (NTV, Channel One, Life News, Channel 24, Zvezda, RIA Novosti, Russia Today,

Rossiya Segodnya, ITAR-TASS, and Komsomolskaya Pravda), as well as Internet publications and agencies (Anna News and Life News) allegedly belonging to the GRU and FSB, are massively involved in this process in Ukraine.

One of the main goals of the Kremlin's disinformation is to shift blame for alleged war crimes committed in Ukraine. For example, when a missile strike by Russian forces hit the train station in Kramatorsk on April 8, killing dozens of innocent people fleeing the horrors of war, Russia blamed Ukraine for the attack.

Some basic principles in misinformation are denial, blame, blame-shifting, and distraction (denial - distraction - blame-shifting). An example of this is the atrocities in Bucha. First, they denied it, then started saying it was provocative. They shift blame and blame Ukraine, and finally, for the distraction, they release similar sadistic videos showing Ukrainian torturers of captured Russian soldiers.

They often use coordinated email trolling operations on Telegram Cyber Front Z, allegedly linked to the "troll farm" that floods the information space with false accusations of war crimes allegedly committed by Ukrainian "neo-Nazis" to drown pro-Ukrainian voices in a sea of lies.

The main narrative of Russian propaganda is that they are not fighting the Ukrainian people but trying to liberate them from a group of neo-Nazis. Naturally, Russia also has its form of mythmaking. Still, it is far less effective since Russian state media, by law, must call the conflict a "special military operation" rather than a war.

The Russians, in 2023, passed several bills and amendments to streamline various state information registries, and the trend is for them to become increasingly closed, with no information from Western citizens available in them.

#### IV. CONCLUSIONS

At the strategic level, the struggle for public opinion in the information space and the protection of critical infrastructure are of utmost importance and have the potential to achieve victory or loss.

This information war proves beyond doubt to people around the world that social media platforms can be successfully used as very effective weapons of mass destruction to create unprecedented disaster in cyberspace. Critical infrastructure, government websites, and social platforms should be strategic assets like diplomacy.

The chronology of the adoption of regulations in the two countries after the start of the war shows that they aimed at securing cyber security at the beginning. Still, one of the first things to be addressed was the protection of e-government and the info security of citizens. Next, measures were taken to counter disinformation and synchronize their media, which is critical to the operation's success.

5G technologies will play a crucial role in future wars, mainly if operating against a more potent adversary with air superiority.

The war shows that the scope of information operations has gone far beyond Russia and Ukraine. It has affected

the whole world. The US, NATO, China, several corporations, significant banks, NGOs, international institutions, and various professional and industry organizations, among others, are involved.

In the end, this analysis shows that Russia is currently losing the information war in the Western world and Ukraine but is having complete success in Russia itself and gaining the understanding of Chinese citizens and other isolated countries such as Iran and North Korea. There have been some partial successes in Asia and Africa, but that could quickly change because the Western powers have much better reach on social platforms like Facebook, Twitter, Instagram, YouTube, and Google.

In the end, it can be said that Ukraine has built modern and very effective cyber units, while Russia is increasingly closing itself off in the Internet space.

#### REFERENCES

- [1] "Про Стратегію кібербезпеки України," Офіційний вебпортал парламенту України, <https://zakon.rada.gov.ua/laws/show/n0003525-16#Text> [accessed Feb. 28, 2024].
- [2] "Про проведення в 2022 році дострокового випуску курсантів випускного курсу Інституту спеціального зв'язку та захисту інформації національного технічного університету України 'кіївський політехнічний інститут імені Ігоря Сікорського,'" Офіційний вебпортал парламенту України, <https://zakon.rada.gov.ua/laws/show/207-2022-%D1%80#Text> [accessed Feb. 28, 2024].
- [3] "Про використання банками хмарних послуг в умовах воєнного стану в Україні," Офіційний вебпортал парламенту України, <https://zakon.rada.gov.ua/laws/show/v0042500-22#Text> [accessed Feb. 28, 2024].
- [4] A. Shevtsov, C. Tzagkarakis, D. Antonakaki, P. Pratikakis, and S. Ioannidis, "Twitter dataset on the Russo-Ukrainian War," arXiv.org, <https://arxiv.org/abs/2204.08530> [accessed Feb. 28, 2024].
- [5] "中睿天下对俄乌网络冲突战略战术的研究分析," 知乎专栏, <https://zhuanlan.zhihu.com/p/486137021> [accessed Feb. 28, 2024].
- [6] [1] "Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України," Офіційний вебпортал парламенту України, <https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text> (accessed Mar. 7, 2024).
- [7] Указ Президента Российской Федерации от 01.05.2022 № 250 · Официальное опубликование правовых актов, <http://publication.pravo.gov.ru/Document/View/0001202205010023?index=3&rangeSize=1> [accessed Feb. 28, 2024].
- [8] "#Russia began active preparations for disconnection from the global Internet No later than March 11, all servers and domains must be transferred to the #russian zone. In addition, detailed data on the network infrastructure of the sites is being collected. pic.twitter.com/wocdrqojej," Twitter, [https://twitter.com/nexta\\_tv/status/1500553480548892679](https://twitter.com/nexta_tv/status/1500553480548892679) [accessed Feb. 28, 2024].
- [9] Указ Президента Российской Федерации от 01.05.2022 № 250 · Официальное опубликование правовых актов, <http://publication.pravo.gov.ru/Document/View/0001202205010023?index=3&rangeSize=1> [accessed Feb. 28, 2024].
- [10] Criminal Code of the Russian Federation from 25.03.2022 <http://pravo.gov.ru/proxy/ips/?docbody&nd=102041891&ysclid=16s7e4gnxa970611260> [accessed Feb. 28, 2024].
- [11] "Хронология военной спецоперации: главные события за первый месяц," Реальное время, <https://realnoevremya.ru/articles/245500-hronologiya-voennoy-specoperacii-30-glavnyh-sobytiy-za-mesyac> [accessed Feb. 28, 2024].
- [12] "Русия започна активна подготовка за изключване от глобалния Интернет," boulevardbulgaria.bg, <https://boulevardbulgaria.bg/articles/rusiya-zapochna-aktivna>

- [podgotovka-za-izklyuchvane-ot-globalniya-internet](#) [accessed Feb. 28, 2024].
- [13] Internet, social networks and VPN, <https://www.levada.ru/en/2022/04/22/internet-social-networks-and-vpn/> [accessed Feb. 28, 2024].
- [14] A. Bougias, A. Episcopos, and G. N. Leledakis, “Valuation of European firms during the Russia–Ukraine war,” *Economics Letters*, vol. 218, p. 110750, Sep. 2022. doi:10.1016/j.econlet.2022.110750 [accessed Feb. 28, 2024].
- [15] Поуки от хибридните бойни действия ..., <https://postvai.com/analizi/hibridni-deistwia.html> [accessed Feb. 28, 2024].
- [16] Vozho, “Какво прави държавата срещу дезинформацията?,” БЛОГодаря, <https://blog.bozho.net/blog/3907> [accessed Feb. 28, 2024].
- [17] Africans in Ukraine face racism from authorities as they escape, <https://www.axios.com/africans-in-ukraine-racism-81bf8ebd-2d03-4373-bdeb-b5de9db7ec91.html> [accessed Feb. 28, 2024].
- [18] F. O. Talabi et al., “The use of social media storytelling for help-seeking and help-receiving among Nigerian refugees of the Ukraine–Russia war,” *Telematics and Informatics*, vol. 71, p. 101836, Jul. 2022. doi:10.1016/j.tele.2022.101836 [accessed Feb. 28, 2024].
- [19] O. B. Okooboh, “Oriana Skylar Mastro on US-china engagement and War in Ukraine,” U.S.-China Perception Monitor, <https://uscnpm.org/2022/04/28/oriana-skylar-mastro-russia-ukraine-china-interview/> [accessed Feb. 28, 2024].
- [20] “Chinese public opinion on the war in Ukraine,” U.S.-China Perception Monitor, <https://uscnpm.org/2022/04/19/chinese-public-opinion-war-in-ukraine/#:~:text=To%20our%20knowledge%2C%20this%20is%20the%20first%20representative, support%20China%20mediating%20an%20end%20to%20the%20conflict.> [accessed Feb. 28, 2024].

# Motivation for choosing an officer career

Grigor Grigorov

Logistic and Technology Faculty  
Vasil Levski National Military University  
Veliko Tarnovo, Bulgaria  
gregari\_@abv.bg

**Abstract.** Changes in the security environment and opportunities in the modern world present increasing challenges for the armed forces of democratic states to staff their structures. The article examines the issues related to the motivation for choosing the military career of an officer. Based on a survey conducted with cadet candidates and a comparative analysis with previous research, the main variables influencing the choice of the officer profession and joining the armed forces are derived. The obtained results could contribute to the improvement of the current system for motivating military personnel and increase the image of the military profession.

**Keywords:** military profession, motivation, personnel

## I. INTRODUCTION

The problem of motivation in modern professional military armies in democratic countries is considered by many authors due to the fact that these organisations face the challenge of recruiting qualified and motivated personnel on par with other employers in the free labour market. Nowadays, due to freedom of movement, globalisation and easy access to information, the opportunities for people of working age are great, and the restrictions imposed by military organisations are often a deterrent to job seekers.

The analysis made in previous studies [15], [16], [17] shows that motivation has a complex structure and is inherent only to the individual or personality, being characterised by a high degree of consciousness [1]. For this reason, it is considered by authors such as Taylor [2], Mayo, Ouchi, Maslow [3], Herzberg [4], Vroom [5], McClelland [6], Skinner [7], Murray, Porter and Lawler [11], Adams, Heider and Kelly, Locke, Kohn [8], Bandura [12], Thomas, Lancaster [13], Pink [9], Lawrence and Nohria [14], etc. Each one of them develops his own theory of motivation and discusses the factors that are predominant in the motivational process. We will focus on a compilation of these theories, deriving the thesis that when looking for a job, external factors related to the working conditions have a predominant influence, while when retaining a job, the dominant influence is the

motivational factors related to the nature of the work itself. External ones correspond to the lower levels of Maslow's hierarchy, and their absence directly affects the choice of occupation because they are visible to the environment surrounding the organisation. Internal ones are related to the specific workplace and lead to an increase in job satisfaction. In other words, a person's satisfaction is the result of the work itself, and dissatisfaction stems from the conditions in which he works. Bad working conditions repel employees, but suitable ones attract them. Routine demotivates them, and interesting work satisfies them. [17]

The aim of the present study is to establish the main motives (factors) for choosing the officer profession and present their importance and interconnectedness.

## II. MATERIALS AND METHODS

The study of the motivation for choosing the officer profession is based on a methodology developed specifically for the needs of the present study, based on data collection by means of a survey. The object of the study is one target group (category) – cadet candidates at Vasil Levski National Military University.

The scope of the research is the number of respondents by category:

- male cadet candidates – 68 persons;
- female cadet candidates – 12 persons.

The total number of respondents is 80.

To achieve the objectives of the empirical research, a questionnaire [19] in Bulgarian was developed. It includes two main parts: the first part – passport, and the second part – questions structured by groups to reflect the opinion of the interviewed persons.

The passport part includes general information about the respondents.

In the second part, nineteen close-ended questions are structured, to which the interviewees should answer. The possibility of giving an answer is in the form of a Likert

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8227>

© 2024 Grigor Grigorov. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

scale, i.e. it is formulated as an assessment with which the respondent may agree (or disagree) to varying degrees.

The scale contains five grades as follows: 1 – very low; 2 – low; 3 – medium; 4 – relatively high; 5 – very high.

Question twenty is open-ended and the respondents can give an answer freely, in the form of a text. The survey was conducted in April 2023.

### III. RESULTS AND DISCUSSION

The analysis of the results of the conducted survey was prepared on individual or group questions from the survey card, considering the opinion of all surveyed categories.

Question № 1 of the questionnaire is formulated as follows:

'To what extent do you feel that the choice of the military profession is personally yours?'

The results for question № 1 are shown in Fig. 1, and their analysis indicates that the majority (95%) consider to a relatively high or very high degree that the choice of the military profession is theirs.

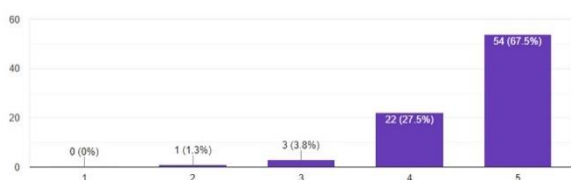


Fig. 1. Response to question № 1

Questions № 2 and № 3 of the survey are phrased as follows:

Question № 2: 'To what extent were you familiar with the character of military activities before joining the Army?'

Question № 3: 'To what extent did your friends or family influence your decision to join the armed forces?'

The analysis of the results for questions № 2 and № 3 indicates that the number of respondents who were or were not aware of the nature of military service before joining the armed forces was approximately the same. Over 32% of the respondents said that their friends and family did not influence their choice of a military career, while over 21% said the opposite. More than 36% cannot give a clear answer, which indicates that the combination of personal motivations in interaction with the opinion of family and friends has led to the intention to make a decision to apply.

Despite the responses given on the interview questionnaire while applying, more than half of the applicants stated that family, relatives and friends connected to the military contributed to or had an influence in relation to the initial impulse to apply.

Questions № 4, № 5, № 6, and № 7 of the survey card concern the prestige of the military profession and the respondents' opinion of its current state and how it has changed over time.

Question № 4: 'To what extent do you think the military profession is prestigious in society?'

Question № 5: 'To what extent do you think the prestige of the military profession is increasing?'

Question № 6: 'To what extent do you think the prestige of the military profession was higher back in time – before?'

Question № 7: 'To what extent do you think the prestige of the military profession is higher now?'

The responses to the questions indicate the unanimous opinion of the respondents (over 92%) that the military profession is prestigious in society. More than 81% of respondents are of the opinion that the prestige of the military profession is increasing, but they cannot express a clear opinion about the comparison of the prestige of being in the military before or now. This shows that the respondents either do not have a good idea of the reputation of military service over the years or the answers they give do not correspond to the specifics of the questions.

Question № 8 of the questionnaire is formulated as follows:

'To what extent do you think the following factors are important in choosing a military career?'

It should be noted that in the article, the concepts of motive and motivation factor are identical.

This question is structured into twenty-one sub-items containing various motives (factors) influencing the choice of a military profession. In this way, the respondents are given the opportunity to indicate what, in their opinion, is the degree of importance of each of the mentioned factors.

Part of the results for question № 8 are shown in Fig. 2, and it is clear from their values that the respondents have put four factors first with almost equal percentages – the opportunity to work in an organisation with clear rules (93%), to work in a team (92%), to serve the homeland (91%), for career development (91%), and second, with the same percentages, are the security and predictability of the workplace and the possibility of working in an international environment (87%), and thirdly – the possibility of working with weapons and equipment (86%), followed by the possibility of wearing a uniform (85%) and receiving free education (over 82%).

In his report, D. Dimitrov wrote: 'Patriotism is a special motive in the activities of military personnel. Without being a patriot, it is impossible to become a reliable defender of the Motherland.' [18], which reflects his opinion that patriotism is one of the main motives for a military career.

The other important motives that are highlighted are the opportunities to participate in missions and operations outside the country (78%) and receiving a good remuneration compensating for the deprivations and adversities resulting from military service (77%). The opinion of those interviewed is also unanimous that important reasons for joining the army are the opportunities for early retirement (76) and the social status of the profession (75%).



If we compare the answers to this question with the results of an identical study [15] (Fig. 3) conducted with Bulgarian military personnel in 2018, obvious differences can be found. In the study conducted in 2018, the factors related to remuneration, early retirement and job security were listed in the first place. The explanation for the discrepancy between the significant factors in the two studies is probably rooted in the fact that in the 2018 study, servicemen had accumulated experience in military service, and the idealistic urges generated by intrinsic motivation were displaced by the absence of purely hygienic factors based on unsatisfied physical needs.

The results of another similar study [17] conducted with over 82% of US military personnel in 2019, shown in Fig. 4, show that the respondents put first the opportunity to participate in missions and operations abroad (80%), and second – the opportunity to serve their country (78%), followed by the opportunity for career development (75%), the opportunity for working with weapons and military equipment (71%), for acquiring free education (67%), for working in a team and in an international environment (65%). The opinion of the respondents is also unanimous that the main motivation for joining the army is remuneration (56%), security and predictability of the workplace (54%), and early retirement (54%, as the right for it in the US armed forces is acquired after twenty years of service).

Comparing the three studies, the internal motivational factors are clearly visible in the studies from 2019 and from 2023. In the study from 2018 with Bulgarian servicemen with experience in the military, they are displaced by the external factors related to working conditions, since they are not satisfied. However, these factors are also evident in the 2019 study with a prevalence of US military personnel, as it is no secret that these factors are the reason many expats and poorer applicants join the military for citizenship, free education, good pay and a number of social benefits. The patriotic motivation expressed by the candidate cadets indicates that they were willing but inexperienced and had not faced with the typical domestic problems of the military. The unrealised announced intake in the last few years shows that internal factors alone are not sufficient to fill the large number of announced candidate cadet places. The efforts of the University management to increase the cadet scholarships have finally been crowned with success, and from the beginning of 2024, they are around the level of the minimum wage for the country. It remains to be seen whether this is a sufficient motivator for entering the military education system, although it alone is unlikely to produce the desired result.

The remaining factors motivating the choice of a military career generally overlap.

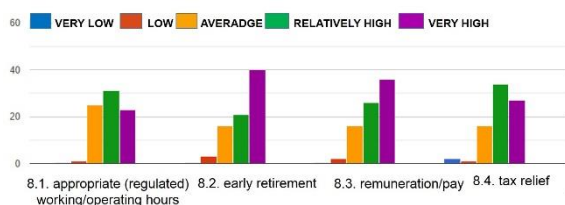


Fig. 2. Response to question № 8 from 2023

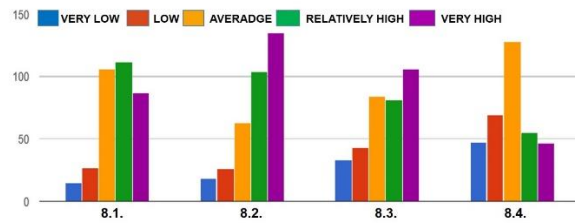


Fig. 3. Response to question № 8 from 2019

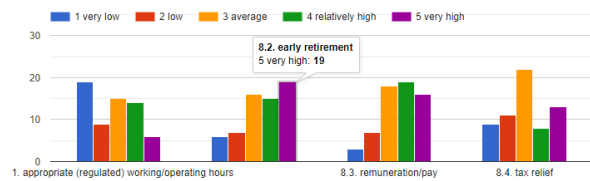


Fig. 4. Response to question № 8 from 2018

As less significant factors for choosing the military profession, the respondents indicated appropriate and regulated working hours, restrictions on personal rights and freedoms, tax benefits and freedom in making decisions at the workplace.

The analysis of the results on this issue shows that the motivation for choosing the military profession is a complex composite of many and various interrelated factors connected with the experience of the interviewees and the specific situation in the armed forces of different countries.

Question № 9 of the questionnaire contains six sub-questions and is formulated as follows:

‘To what extent do you feel you received information about applying to the University/armed forces from the following sources?’

From the answers given (Fig. 5) on this question, we can conclude that the main sources of information are the website of the organisation/Military University (73%), followed by the information provided by family and relatives (58%), friends (51%), and advertising campaigns in schools, ‘Be a soldier’, etc. (43%). It should be mentioned, however, that the initiating information comes primarily from people connected to the military, such as relatives, close people, and friends, and only after an interest in the military profession has been provoked, information is sought on the University’s website. This means that the public is not aware of the possibilities of service in the armed forces and the nature of the military profession.

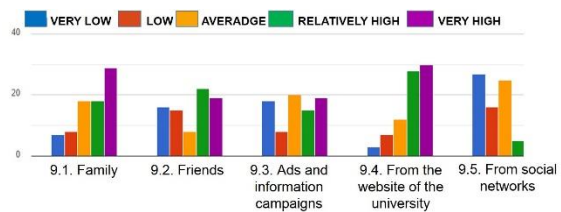


Fig. 5. Response to question № 9 from 2023

Question № 10 of the questionnaire is formulated as follows:

‘To what extent do you think that the frequent legal changes regulating the conditions for exercising a military profession influence the personal choice to enter the University/armed forces?’

The results of question № 10 indicate that almost 34% of the respondents consider the negative impact of legal changes in the army. The answer to this question shows that the respondents do not yet have the experience and the necessary information to give an unequivocal answer.

Questions № 11 and № 12 of the questionnaire concern the interrelationship between the choice of the military profession and resource provision, the state of armaments, equipment and infrastructure. The questions are phrased as follows:

Question № 11 – ‘To what extent do you think that interest in the military profession has decreased due to systematic and insufficient resource provision?’

Question № 12 – ‘To what extent do you think that interest in the military profession has decreased due to obsolete equipment, weapons and infrastructure, and the delay in their modernisation?’

The results of question № 11 show that almost 38% of respondents believe that resource provision is insufficient, which adversely affects motivation in the military. Comparing the responses given to this question with those from the 2018 survey, it is not difficult to spot the difference. In 2018, over 80% of the Bulgarian military stated categorically their dissatisfaction with resource provision [17]. In many cases, this leads to the demotivation and departure from the military of qualified personnel faced with the adversities of military service caused by the lack of material resources.

Comparing the responses to question № 12 of the 2023 survey with that of 2018, the differences in opinion contrast very strongly. In the survey from 2018, the respondents were categorical (more than 75%) that the morally outdated equipment, armament and infrastructure as well as the delay in their modernisation lowers the interest in the military profession. The responses to the 2023 survey of officer candidates are the opposite – over 31% of the respondents agree that motivation is not affected by modernisation. Candidate cadets still have no real idea of the actual state of the equipment and its provision; therefore, their motivation cannot possibly be at a low level or negatively affected.

Question № 13 of the questionnaire is formulated as follows:

‘To what extent do you think civil-military relations in your country are effective?’

The results on this question indicate that the respondents cannot give a definite opinion on it. This could be due to poor awareness of the issue of civil-military relations or taking them for granted at the level they are – average.

Question № 14 of the questionnaire is formulated as follows:

‘To what extent do you think that if the relationship between the public and the military improves, interest in the military profession will increase?’

From the results of question № 14, it is clear that about 83% of the respondents are consolidating around the opinion that interest in the military profession is directly proportional to the strength of the ‘society-military’ relationship. The results of the studies conducted in 2018 and 2019 are similar.

Questions № 15, № 16, № 17, and № 18 of the questionnaire are related to the popularity of the military profession in society.

The questions are formulated as follows:

Question № 15: ‘To what extent do you think the public is aware of the activities of the armed forces at this time?’

Question № 16: ‘To what extent do you think a military career is popular in society?’

Question № 17: ‘To what extent do you think the media needs to promote the military profession?’

Question № 18: ‘To what extent do you think civilians are aware of military career opportunities?’

The analysis of the results of the questions shows that the majority of the respondents (more than 42%) believe that the public is not familiar with the activities of the military at the moment, and about 39% cannot give an unequivocal answer.

The answers to question № 16 show that over 41% of respondents are of the opinion that a military career is popular in society, and again, there is a great percentage of those who cannot judge (38%).

The majority of respondents (75%) are of the opinion that the media should be actively used to popularise the military career because the public is poorly informed about the possibilities of practicing it. Almost 40% of the respondents are of the opinion that civilians are not aware of these possibilities, and 35% cannot judge.

The analysis of the results of these questions in this and the previous studies are identical and show that there is a need to improve the ‘society-military’ relationship, which would lead to an increase in interest in the officer and military profession in general.

Question № 19 of the questionnaire is related to satisfaction with the choice of the military profession.

Question № 19: ‘To what extent do you think choosing a military career will meet your expectations?’

From the analysis of the results of the questions, it can be said that the majority of respondents (81%) are of the opinion that a military career will meet their expectations. The answer to this question indicates that cadet applicants have high expectations for the military profession, but subsequently they have to be justified or rejected.

Question № 20 is open-ended and is worded as follows: ‘In your opinion, what would motivate you to join the army today?’

Most candidates gave an answer to this open question.

Some of them are as follows: ‘Desire for the profession and love for the country.’, ‘Improving personal qualities.’, ‘Serving your country and wearing a uniform.’, ‘Secure work.’, ‘Security in the profession and pay.’, ‘The

opportunity for development and the hierarchy.’, ‘Wearing a uniform.’, ‘The military provides many opportunities for career development and secure employment after graduation.’, ‘The order, discipline, security and organisation.’, ‘The fact that I will serve the country motivates me, the secure career, early retirement and many other benefits.’, ‘I am motivated by the choice to develop in BAF through Vasil Levski NMU.’, ‘Because I want to serve my country.’, ‘Work in the service of the nation.’, ‘I am motivated by the order and discipline in this environment.’, ‘I am motivated by the fact that I will serve the country and have a safe and a good job.’, ‘Opportunity for career development and on a personal level as well.’, ‘Patriotism and the great scope for realisation in the country and abroad.’, ‘The military provides opportunities for development that civilian life does not offer.’, ‘The privilege to serve my country.’, ‘Career and personal development, building new relationships and friendships, getting a quality education.’, ‘The opportunity to serve my country and career development.’, ‘I am motivated by the fact that serving in the military is vocation and responsibility.’, ‘The sense of duty to the country, new friendships and the fulfilment of a childhood dream to study at NMU.’, ‘What motivates me is that all my relatives had access to government jobs, specifically the security we get after graduation. For me, wearing a uniform is an honour and a dignity.’, ‘Getting a high-level education and good realisation.’

The analysis of the results on this question shows that, in the first place, more than 2/3 of candidates indicate the patriotic reasons for joining the army, such as service and duty to the country. Workplace security, discipline and order are listed in second place. In third place in the hierarchy are the good opportunities for career development and receiving free education, followed by early retirement, wearing a uniform, the opportunity to build new friendships, work in a team, etc.

As less important motives, character building and desire to try something new and different, work with clear rules, desire to work in an international environment, etc. are mentioned.

The results of the conducted research led to the following conclusions:

The choice of the officer profession is individual and conscious, but often family and friends are the ones who contribute to it by sharing information, experience and family traditions. The majority of those interviewed shared that they are familiar with the nature of the officer and military profession in general, it is prestigious, but not popular in modern society. It is necessary to increase the awareness of it, as well as the opportunities to do it.

The analysis of the motives for choosing an officer’s profession puts the factors related to the nature of the work itself in combination with patriotic motives in the first place, and the factors characterising the workplace in the second place. Of particular importance are remuneration, opportunities to participate in operations outside the country, and social benefits. The comparative analysis of this study and the study conducted in 2018 shows that first-hand information, through accumulated experience, changes the motivational structure, placing first the external factors describing the specific workplace

and the organisation, and second – the internal factors related to the nature of the work itself. That is, in order to reach the internal motivation, it is necessary to go through the external one, corresponding to the factors from the lower levels of Maslow’s pyramid. When the satisfaction of these factors is reached, motivation through the work itself is inevitable, and physical motives begin to lose their importance.

There is a similarity with Galbraith’s theory about the influence of the system of motives – compulsion; monetary remuneration; identification; adjustment. In his research, Galbraith found that a paradox related to the monetary motive occurs: ‘The higher the level of remuneration, the less its value relative to other motives.’ [10] He finds the explanation for this not in the decreasing and insignificant value of money, but that with the increase in income, in most cases, the dependence on the specific workplace decreases. At the same time, the element of compulsion will also decrease, leading to identification with and adjustment to goals and devaluation of money as a motive.

The studied factors show that motivational behaviour has a complex structure and is influenced by the awareness of job seekers. The more informed they are about the nature of the work and the characteristics of the workplace, the more informed choices they will make.

The analysis of questions related to civil-military relations confirms the linear dependence of the strength of the ‘military-society’ connection and the interest in the officer profession. The officer and the military profession in general are not desirable nowadays despite the conflicts in Europe and the Middle East. Popularisation is needed by conducting media and information campaigns with the aim of popularising it and raising its prestige.

It is necessary for those in power to realise that the officer and military profession in general in peacetime is a profession like any other, and apart from patriotic motives and the nature of the work itself, it must be financially, materially and socially secured in order to be competitive in the labour market. Modern generations have different perceptions of the world and expectations of work. They hardly tolerate limitations and want goals to be achieved quickly, leading to the desired end result. The conducted research shows that the profession of an officer is still prestigious, but contrary to this statement, the applicants for it and for joining the armed forces are decreasing at an alarming rate. It is necessary to build a motivational model for attraction and retention in the armed forces, which takes into account the modern realities of the labour market combined with the changed expectations of new generations. Everyone knows the saying, ‘A nation that does not feed its own army will end up feeding a foreign one!’, but the problems are still swept under the carpet.

#### IV. CONCLUSIONS

The analysis of the results of the conducted research shows that the choice of an officer’s career is independent, but is influenced by the opinion of family and friends. The officer profession is losing its popularity in society and there are fewer and fewer candidates for it. The motivation for its choice has a complex structure composed of various external and internal motives

(factors). In the first place, the factors related to the nature of the work itself stand out in combination with patriotic motives, and secondly, the factors characterizing the workplace. Of particular importance are the remuneration, opportunities to participate in operations outside the country and social benefits. Each of these motives alone cannot solve the problem of motivation. An up-to-date interrelated model needs to be implemented, comprising all the main motivational variables, in order to fill the shortage of personnel not only for officers, but for military personnel in general.

In today's globalised information society, motivating staff is a difficult task. All information is one 'click' away, and if one wants to attract motivated and qualified personnel, meeting the needs of the military organisation, one should meet the expectations of job seekers. The problem of the lack of officers is getting worse and will not tolerate delay. Immediate action is needed to fill the growing vacuum and build a modern military to meet the threats in today's security environment.

#### ACKNOWLEDGMENTS

The publication of the article was financed with funds provided by the National Security and Defence Science Program.

#### REFERENCES

- [1] Иванов, И. Организационна психология, Велико Търново, Фабер, 2005, с. 172.
- [2] Ангелов, А., „Основи на мениджмънта“, Тракия – М, С., 1998, с. 189- 190
- [3] Maslow, A., Motivation and Personality, Harper & Row, 1970
- [4] Herzberg, F., One more time: How do you motivate people, Harvard Business Review, 1968
- [5] Vroom, V., Work and motivation, Wiley, New York, 1964
- [6] McClelland, D., That urge to achieve, Management Classics, 1986.
- [7] Skinner, B., Contingencies of Reinforcement, Appleton-Century-Crofts, New York, 1969
- [8] Kohn, A., Punished by Rewards: The Trouble with Gold Stars, Incentive Plans, A's, Prizes and Other Bribes, Boston: Houghton Mifflin, 1993.
- [9] Pink, D., Drive: The Surprising Truth About What Motivates Us, New York, 2009.
- [10] Galbraith, J., The new Industrial State, Princeton university Press, First Princeton Edition with a new foreword by J. Galbraith, USA, 2007, p. 167
- [11] Porter, L., Lawler, E., Managerial attitudes and performance, Homewood, Ill., R.D. Irwin, 1968.
- [12] Wood, R., Bandura. A., Social Cognitive Theory of Organizational Management, The Academy of Management Review, Vol. 14, No. 3 (Jul., 1989), pp. 361-384.
- [13] Lancaster, L., Stillman, D. When generations collide: Who they are. Why they clash. How to solve the generational puzzle at work. New York, NY: Harper Collins. 2002.
- [14] Lawrence, P., Nohria, N., Driven: How Human Nature Shapes Our Choices, San Francisco: Jossey-Bass, 2002
- [15] Grigorov, G., Spiridonov, S., Research on the Motivation for Choosing the Military Career, The 24th International Conference The Knowledge-Based Organization 2018, conference proceedings 1 , p. 302 – 307, Nicolae Balcescu Land Forces Academy, Sibiu, Romania, 2018, Available: <http://dx.doi.org/10.1515/kbo-2018-0048>
- [16] Grigorov, G. Lilov, L., Structure of Motivation for Training in Engineering Specialties, ENTerprise REsearch InNOVation Conference SPLIT, CROATIA, IRENET, Society for Advancing Innovation and Research in Economy, Vol. 4, No. 1, pp. 388 – 396, Zagreb, Croatia, 2018, Available: <http://dx.doi.org/10.2139/ssrn.3283730>
- [17] Grigorov, G. Motivation for Choosing and Practicing the Military Profession, The 26th International Conference The Knowledge-Based Organization 2020, conference proceedings: 2 , pp. 162 – 169, Nicolae Balcescu Land Forces Academy, Sibiu, Romania, 2020, Available: <http://dx.doi.org/10.2478/kbo-2020-0070>
- [18] Димитров Д., „Основни мотиви за воинска дейност“, Годишник на НВУ „В. Левски“, В. Търново, 2016.
- [19] Проучване за изследване на мотивите за постъпване на военна служба, Available: <https://docs.google.com/forms/d/1IDXthlTlyN88PBkuDBxvagDhujV5Dtxhgr7ujFjs1ws/edit#responses>

# *Model for Recruiting Servicemen in the Armed Forces*

**Grigor Grigorov**

*Logistic and Technology Faculty  
Vasil Levski National Military University  
Veliko Tarnovo, Bulgaria  
gregari\_@abv.bg*

**Abstract.** In the decades of transition from conscript to professional armed forces, a number of unforeseen issues arose for the armed forces. One of the unresolved, but the most important and worrisome among them, is how the armed forces can attract and retain motivated personnel from the open labour market to fill the vacancy vacuum. Based on conducted research on the motivation of military personnel, the article examines a model for attracting them in the armed forces, analysing each of the elements that make it up and the interrelationships between them. This will contribute to enriching existing knowledge about work motivation and developing strategies for attracting and retaining military personnel.

**Keywords:** *armed forces, motivation, recruiting, servicemen.*

## I. INTRODUCTION

In recent decades, employee motivation has been an issue of increasing importance. The military is no exception to the problem, and in it, the issues related to the shortage of qualified personnel are common to organisations in the private sector.

A review of previous research [1], [2], [3] on the issues of motivating military personnel showed that problems with personnel motivation concern two main areas: the attraction of military personnel and their retention in military service. Each of these areas embodies a component of the general motivation of military personnel; thus, they should be considered interrelated. The specificity of the activities and the complexity of the factors in each of the components requires its separate consideration for a more detailed and understandable description of its constituents. Therefore, one of the components will be proposed and described in the current work – the model for attracting military personnel, and in the next one, the model for retention in the armed forces.

## II. MATERIALS AND METHODS

Based on the analysis of the theoretical and practical experience of the conducted researches [4], [7], [8], a model for motivating candidates to join the armed forces is proposed. The model is presented in Fig. 1 and illustrates the factors influencing the behavioural choice to enter the armed forces that can predict and influence the behaviour of job seekers.

## III. RESULTS AND DISCUSSION

The model is borrowed from proposals in the NATO study [13] and adapted to the specifics of the Bulgarian Armed Forces. In this model of motivation to enlist, the behavioural variable is called ‘job search’. Job searching can take many forms (e.g. applying, accepting a job offer, completing initial military training, etc.), depending on the potential candidate’s stage of employment. According to this model, a person’s intention to act is assumed to be the immediate antecedent of his behaviour, and this intention, in turn, is predicted by the degree to which a person has a positive or negative attitude toward the search. The model also accounts for various indicators that are hypothesized to be determinants of candidate attraction. These indicators refer to people’s personal characteristics (beliefs, perceptions, expectations) and are believed to influence behaviour and/or intention. The model further relies on principles from information and communication theory [9]. Applied in the context of recruitment, communication can be represented as conveying a message to a target group of (potential) candidates through a specific source or medium [5]. The content of the message refers to information about the available jobs (e.g. type of work to be performed, level of pay) and the seeking organisation (size, type, industry), which may play a crucial role in the decision-making process of the people. The message is usually conveyed

*Print ISSN 1691-5402*

*Online ISSN 2256-070X*

<https://doi.org/10.17770/etr2024vol4.8228>

© 2024 Grigor Grigorov. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

and controlled by the organisation seeking to recruit and attract new employees. In addition, people receive information about the organisation from other sources

(e.g. word of mouth, general public), not all of which are under the direct management of the organisation.

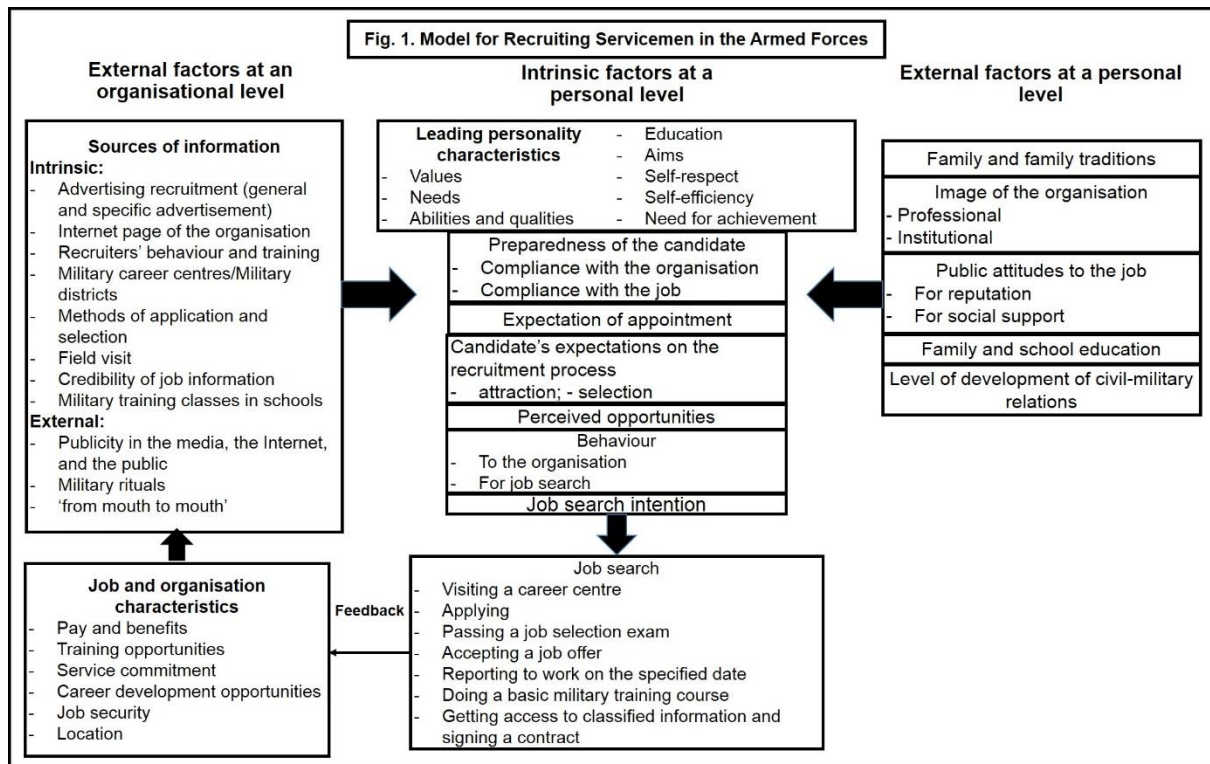


Fig. 1. Model for Recruiting Servicemen in the Armed Forces

The analysis of the results on this issue shows that the motivation for choosing the military profession is a complex composite of many and various interrelated factors connected with the experience of the interviewees and the specific situation in the armed forces of different countries.

Ultimately, personal choice depends on the decisive impact of the personal characteristics distinguishing individuals (values, needs, education, goals, etc.) and guiding their behaviour in the recruitment model. Each factor or group of factors in the model is described and supported by theoretical or empirical data from military or civilian sources. When describing the model, we will focus attention not only on the individual constituents, but also on the connections between them.

**Components of organisational attractiveness**

In general, recruitment efforts influence people’s behaviour by providing them with application information, referrals to the organisation, visiting the organisation’s website or on-site. In the current model, 'job search' is used to link to different possible behaviours. Some of the application behaviours occur in the initial stage of recruitment while others, such as accepting a job offer, are typical of the later stages of recruitment. When considering the military recruitment system, we identified the following stages: attraction, application, individual training, and acceptance into military service. Refracted through the prism of the considered model, these stages include: attempts to persuade potential candidates to visit

military career centres (military districts, reception centres) and to apply for military personnel (attraction); attempts to retain interested candidates by encouraging them to submit application documents, participate and win a competition (application); and finally – persuading the willing candidates to accept the offered position in the military and report to work on the specified day of entry (acceptance into service). Individual training is an element that, according to the current legislation [14], is carried out after signing the contract for military service, with a clause for termination in case of unsuccessful training.

Going through this recruitment cycle, candidates acquire new information about the organisation through various sources. This emphasizes the importance of having a feedback element in the model to ensure that information about the organisation is received and updated in the recruitment process. The forms for receiving feedback are different. An option is filling out a survey in case an applicant renounces at any stage of the application process. In addition, in order to obtain up-to-date information about the entire recruitment system, a survey of the opinions of everyone who has passed through the system and entered the service is imperative. The analysis of the information obtained could be used to improve the system and maintain active feedback on the overall recruitment process.

**Factors affecting the search for a military profession**

In the model, predictive factors are distinguished at the organisational level and at the personal level. Organisational-level factors refer to the real environment in terms of organisational and work characteristics. Personal-level factors refer to the perceived environment, in terms of the individual's subjective interpretation of work and organisational characteristics. Most of the job search factors can be classified according to 'implicit theories' of job selection by Behling, Labovitz and Gainer [10] as: objective factors, subjective factors, and critical review of the organisation's information sources. The objective factors approach suggests that job search decisions are based on an assessment of the advantages and disadvantages of objective job indicators and organisational attributes (e.g. salary, type of job, size of organisation). Objective factors are related to the real environment. The subjective factors approach suggests that job search is based on the perceived confluence between the individual (e.g. personality characteristics, needs, values, education) and the image of the organisation (professional and institutional). They refer to the subjective interpretation of the organisation based on available information. In considering the recruiting model, objective factors will be taken as equivalent to organisational-level factors, and subjective factors will be treated as equivalent to personal-level factors. A critical view of organisational information sources suggests that potential candidates often have insufficient information to make informed job choices, so they rely on early recruitment contacts to discriminate between organisations.

In recruiting, the main role is played by the characteristics of the organisation and vacant jobs. In considering these types of characteristics, we will pay particular attention to their impact on attracting candidates. It should be noted, however, that individuals make important distinctions between job attractiveness and organisational characteristics. A leading role in the candidate's behavioural choice is given to the internal personal characteristics (needs, values, abilities, qualities, education, etc.), which will be considered subsequently.

#### **Characteristics of the organisation and work**

The analysis of the results of the conducted research on the motivation for choosing a military profession convincingly showed the importance of external factors in the form of organisational characteristics, such as the amount of remuneration, early retirement, security and predictability of the workplace, etc. In addition, internal factors related to patriotic motives, value system, personality characteristics, and unsatisfied needs have a significant influence on the choice of profession. It should not be forgotten that external factors are the basis for the emergence of internal ones. Therefore, without external incentives, dissatisfaction would arise in the individual, leading to an inability to generate genuine internal motivation, which would make attracting and later retaining personnel impossible.

Many organisational characteristics are visible and discoverable to the majority of job seekers. At the beginning of the job search process, in case organisational characteristics are not visible, they can be found relatively

easily through recruitment advertisements and brochures in electronic and print media as well as in the Employment Agency. Therefore, job seekers use organisational characteristics to screen their potential job opportunities within the organisation before looking at specific vacancy characteristics. This means that candidates first choose from among possible fields of activity depending on their abilities and attitudes to the respective industries, and only after choosing some of them, they start looking for vacancies in the chosen field. In other words, organisational characteristics can act as indicators of organisational values and culture and, therefore, influence a job seeker's decision by repelling or attracting him.

The specified organisational characteristics were considered in the analysis of the results of the conducted researches [7], [4]. The summarised results of these studies indicate the dominant importance of early acquisition of the right to pension, the amount of remuneration, security and predictability of the workplace, opportunities for improvement and career development, suitable (regulated) working hours, obtaining free education for cadets, and the possibility to work with armaments and military equipment. Each of the mentioned factors has a different importance for potential candidates, but their overall impact plays a significant role in the attraction process, which is why it is necessary to periodically review, improve and present them.

#### **External factors at the personal level**

Perceptions of organisational characteristics are influenced by personal and social understandings of the particular organisation. Speaking of the military organisation, the attitude of the person is tied to the level of development of civil-military relations. It is impossible that the personal image of the organisation does not have a historical institutional encumbrance related to the traditions of honouring the military in the country. The stronger the 'society-armed forces' relationship at a given moment, the better individual attitudes toward the armed forces organisation.

**Organisational image** comprises two main subgroups of factors: professional and institutional. The institutional ones describe the organisation itself and include service prestige, innovation, historical traditions, honour, respect, professional values, discipline, etc. The professional ones are primarily focused on the specific occupation and contain pay and security, career development opportunities, benefits and compensation upon leaving, retirement opportunities, professional training, opportunities for attractive personality expression, adventure and travel, benefits, etc. The information about the listed subgroups of factors builds the candidate's perception of the organisational image. Therefore, the more accessible and adequate it is in society, the more likely it is that more people will build an accurate image of organisational opportunities and at a certain point be motivated to apply to the organisation, in case their image coincides with the understanding of desired job.

**Family and family traditions** in the pursuit of a profession often occupy an important, if not leading, position among the factors determining the choice of a

profession. No one would be surprised by the news that the doctor's son is a doctor, the lawyer's son is a lawyer, or the engineer's son is an engineer. For many people, the opinion of the family is decisive in forming a decision. Affiliation with an organisation is in many cases determined through our friends and relatives working in that organisation. People feel much more empathetic and interested when they are connected to the organisation through family, relatives or friends. Practice shows that not a small part of active military personnel in Bulgaria have family burdens and, in one form or another, family members, relatives and friends connected with the military have an influence on the choice of profession.

**Public attitudes** towards a certain profession in many cases play a significant role in its choice. These attitudes are usually the embodiment of the organisational image in society and the organisational reputation. Image does not include an evaluative component from society and refers to a person's own beliefs about the organisation, while reputation refers to people's (general public's) evaluation of the organisation in comparison with other organisations. Therefore, reputation focuses on aspects of an organisation refracted through the prism of the social subjective component and can be both positive and negative.

Personal perceptions of organisational image are based on the experience and background an individual has in relation to the particular organisation. They represent his personal judgment about it and whether the particular organisation is famous or infamous. Public reputation of an organisation encompasses the opinion of a wide group of people about an institution, and often individual judgments are influenced by those of the general public.

Organisational reputation is built over a long period of time and should be an obligation for everyone directly involved in the organisation. Often, single actions of individual members of the organisation discredit the public trust and image of the entire organisation.

In different historical periods, the image of the organisation may be different under the influence of a number of factors. The summarised results of the conducted research indicate that the respondents consider the military profession to be prestigious in society. However, the majority of them are of the opinion that nowadays the prestige of the military profession is much lower, and not enough is being done to promote it. This brings the need for action by all involved in the organisation to reverse the trend of organisational prestige from decline to growth.

**Education** invariably accompanies individual development. Two main factors influence the process of personality building: individual aptitudes and surrounding environment. The first component includes the set of potential opportunities for the development of a person and mainly affects the type of temperament (related to the type of higher nervous activity) and the capacity for physical and mental development. These components of individual development are the preparation for modelling the future personality, but the tools for this modelling

include the set of factors under the influence of external environment. The main place among them is family education and depending on its positive or negative direction, the other constituents of the surrounding environment can act as catalysts or inhibitors. Children are plasticine modelled in the hands of parents; therefore, the responsibility for their upbringing is huge. Some parents try to attribute some of their irresponsibility to educational institutions and the outside environment, but the truth is that without family support, certain actions or inactions have no future.

Educational institutions are a significant factor in the surrounding environment, especially in the early years of a person, and have a significant contribution to individual development. Expanding personal ideas, enriching knowledge, and education in social values are one of the main tasks of schools.

In order to familiarise the public with the activities of the armed forces and improve the public's awareness of national defence activities, with the adoption of the Law on the Reserve in 2013, the preparation of secondary school students for the defence of the country was regulated: "Citizens of the Republic of Bulgaria in the two stages for acquiring secondary education are trained to acquire knowledge and skills related to the defence of the homeland, survival actions in crises of a military nature, as well as the missions and tasks of the armed forces [15]. The training takes place within 5 study hours for the tenth grade and 5 study hours for the eleventh grade, in the classes of the class teacher, on the specific topics set by a regulation of the Council of Ministers [16]. The classes provide general information to the students about the activities of the armed forces and the other departments with regard to the defence of the fatherland, while at the same time providing a good opportunity to improve patriotic education. The limited time does not provide an opportunity to give comprehensive information, but it gives a good basis for initiating motivation to search for further information and a possible choice of the military profession.

The remaining factors forming personality upbringing depend on the specifics of the environment surrounding the particular person. Depending on their combination, the personality builds a certain affinity for the military profession and an overall image for the military institution. Subsequently, if the military itself provides sufficient up-to-date and accessible information to the individuals, it will influence to a certain extent their attitudes towards seeking employment in the military organisation.

#### **Internal factors at the personal level**

**The leading personal characteristics** are a set of the formed value system, active needs, qualities and abilities of the person, their education and goals. Depending on the development of these variables, the individual becomes a person with a unique individuality. On the basis of previous experience and individual development, the person builds a system of personal decision-making



criteria, which is why the importance of each of the listed variables can prevail at a certain point in time.

The development of an individual value system is directly related to family upbringing and traditions, the folk psychology of society, school education, the environment in which a person grows up, and the dominant social values of the specific historical period. Subsequently, the developed value system, in combination with the level of education and other leading factors, plays a significant role in the decision to support the intention and later – in the job search behaviour.

It is necessary to know that the degree of education possessed by the individual is of essential importance in the further development of the value system. In the evolution of motivation, there is a direct relationship between the three variables: behaviour – value system – education. The strength of the volitional response prohibits or permits a certain behaviour, but the choice of a certain behaviour is directly dependent on the previously developed value system of the individual. The value system itself is formed both by family upbringing and the surrounding environment and by the education of an individual. Therefore, the higher education an individual gets, the more his value system changes and develops, shifting the values of the different value levels.

This leads to the conclusion that the motivation for choosing a certain behaviour is directly related to the degree of education of the person.

**Candidate preparedness** is an important aspect of making the decision to look for a job and choosing a certain behaviour when applying. Based on the assessment of own abilities and available information about the organisation, the individual evaluates the correspondence between individual characteristics and organisational requirements and those of the specific job. The correspondence assessment includes two components – correspondence with the organisation and correspondence with the specific position. Depending on the result of the assessment, the possible options are:

- compliance with the organisation and position;
- compliance with the organisation, but non-compliance with the position;
- non-compliance with the organisation, but compliance with the position;
- non-compliance with the organisation and position.

The specified options are not unique and a combination of each of them is possible.

Seen through the interpretation of Maslow's theory of hierarchy of needs, it would be more acceptable to consider a certain percentage correspondence between personal characteristics and organisational-job requirements. When the percentage correspondence is in favour of individual characteristics, the likely personal decision is to proceed with applying for the desired position. Otherwise, with an increased percentage discrepancy, the likelihood of application intention and behaviour occurring is low, but not impossible. Rather, the desire to try a new venture or the impact of other subjective factors would tip the scales towards the choice to apply. In this case, however, the possibility of later

voluntary refusal is high, due to a possible discrepancy with the expectations upon entry into service.

Candidates' preparedness may be enhanced as a result of individual efforts to effect change. When it comes to improving certain physical abilities and mastering certain knowledge by a physically fit person, achieving this is a matter of personal desire and attitude. When there are inconsistencies in the requirements for physical and mental fitness and insufficient mental capacity, then achieving organisational-job requirements is almost impossible.

**The expectation of appointment** is a function of the personal judgment made for organisational-job compliance. According to Vroom's expectancy theory, people choose among a set of job options based on the motivational strength of each alternative. Motivational strength is a function of the product of expectancy (the individual's beliefs that he or she will be successful in obtaining the job), instrumentality (appraisal that the effort will lead to the specified reward/goal), and valence (the personal value of the reward/outcome). That is, a person is motivated to apply to the extent that he/she believes that their efforts will lead to passing the application exams (expectancy), this will lead to a reward – accepting a job (instrumentality), and the value of the job is strongly positive (valence). Therefore, according to the expectancy theory, it can be argued that positive job expectations are predicted to lead to more effort being put into finding a job.

A number of studies have been done to support the above statement. Collins and Stevens found that 'hire expectations are strongly related to applicant attraction and application intentions' [11]. Another study in 2005 found that 'hire expectations can predict job choice and are linearly related to job search attitudes.' [12] The results of these studies confirm the importance of realistic expectations and the importance from having up-to-date and accurate information about the application process and job expectations with their advantages and disadvantages.

#### **Sources of information**

A critical view of organisational information sources suggests that applicants' job pursuit decisions are based on their interpretation of various aspects of the recruitment and selection process (e.g. characteristics of the recruiting organisation, understanding of selection practices). In the absence of other information about the organisation, applicants interpret the information they receive in the application process to gain insight into the work in the organisation.

The recruitment process is a series of logically related steps of attraction, application and acceptance. Each of them has its importance, but all of them are related to the individual's decision of intention and job search. Sources of information are at the heart of informed choice and can influence candidates' job search decisions. Through information, the organisation can influence the general public, attracting or repelling job seekers. This gives reason to consider information about the organisation as one of the main tools for influencing behavioural choice.

Depending on the place relative to the organisation, we can classify information sources as internal and external. Internal sources include: recruitment advertising (general and specific advertising), organisation website, conduct and training of recruiters, military career centres/military districts, application and selection methods, site visit, reliability of job information, classes with military training in schools. External sources include: information in the media, the Internet and the public; attendance and coverage of military rituals; word-of-mouth information.

**Internal sources of information** are largely under the control of the organisation and are used to disseminate official recruitment information to potential candidates. External sources of information are difficult to control by the organisation and generate information available to the general public. We will briefly review some of the most important information sources.

Advertising refers to general and specific advertising. General advertising aims to create a positive attitude towards the organisation, while specific advertising is related to the specifics of the given job. Given the capabilities of the Bulgarian Armed Forces to conduct expensive information campaigns for recruitment in the media, advertising decisions come down to conducting advertising with one's own forces and means. The 'Be a soldier' campaign is traditionally carried out by the Bulgarian Armed Forces. It combines both general and specific advertising as much as possible, providing positive signals to the general public and specific information about job vacancies. This campaign takes place in the regional towns, but the study of the motivation for choosing a military profession indicates that a significant number of candidates join the army to escape unemployment in the small town. In large cities, the chances of attracting more potential candidates are greater, but there the average level of remuneration is higher, which creates conditions for increased competition from private organisations looking for personnel. This reduces the chances of campaign success, especially in large cities, where realisation in the private sector offers much better prospects.

An option to attract the young generation is the use of social networks, advertising videos on YouTube, Vbox and elsewhere. The clip produced by private Stanislav Yotovski with the name BULGARIAN ARMED FORCES 2017 – GLORY LASTS FOREVER! [17], after the NATO exercise 'Saber Guardian – 2017' in Bulgaria, gained wide popularity. There is a need to create and use more such videos and promote the activities of the armed forces to the general public.

To recruit cadets, annual candidate cadet campaigns are held in many schools in towns across the country. They confirm the authority of the Bulgarian Armed Forces as a desirable employer, but they are mainly aimed at officer candidates. It is possible to run such campaigns for soldiers outside of the 'Be a Soldier' campaign. With a little resource and greater desire, any formation

commander can implement activities to promote the military profession and fill their vacant positions.

The next major source for advertising is the organisation's website. In today's digital society, almost everyone has access to a computer, smartphone, and the Internet. For the youth, it is a way of life with which they are inextricably linked. Searching for work on the Internet has been popular for a long time. Traditional print job ads have been supplanted for years by job posting sites. The favourites among them in Bulgaria are jobs.bg, zaplata.bg, rabota.bg, and the Employment Agency of the Ministry of Labour and Social Policy (az.government.bg). The Ministry of Defence maintains up-to-date information for job seekers, and each competition is published not only on the website of the Ministry, but also on the website of the Employment Agency. Potential candidates can get an idea of the job requirements, but not the specifics of the job. This necessitates providing a contact for feedback and questions in order to provide quick and accurate information to potential candidates.

Another recommended requirement is that the information on the websites of the military formations be up-to-date and accessible from a smartphone. They have established themselves as the new information medium, so sites need to match their support requirements. The rest of the organisational information also needs to be up-to-date, in case the candidate wants to become familiar with the functions and structure of the future workplace. It is not an isolated case that a person comes across a non-existent organisational structure or that it is impossible to find information about employees, procedures and up-to-date regulatory documents. The organisation's website is the main source of information, which is why the application information there needs to be up-to-date and easily accessible.

The next unit of the military information system is the military districts. They serve to establish the first contact with potential candidates. Their goal is to consult and attract the required number of candidates for military service. Military districts exist in every regional city, and in the municipal centres, subordinate sectors to the regional military districts exist, usually located in the buildings of the municipal administration. The main function of military districts is to organise the keeping of the military record in peacetime and wartime as well as the distribution and assignment of mobilisation tasks. In addition, military districts carry out tasks related to popularisation of the military profession, training in higher military educational institutions, training of Bulgarian citizens in courses, and training of civilians and those serving in the reserve. The network of military districts was built at the time of the operation of the conscript army, and after its replacement by a professional one, they continued their activity. Military districts are places where interested candidates can get the necessary information about the military profession, vacancies and how to apply. In addition, at these places, assistance is provided in completing the necessary documents and sending them in due order.

Field visits are an excellent way to get a first-hand look at military discipline and to gain a general understanding of specific military formations and the military as a whole. Visits to military formations are organised on open days of military holidays, organised visits for familiarisation purposes and during military rituals of the troops. The specificity there is that only positive information is presented and what is planned to be seen. With them, it is difficult to notice some negatives of the service, unknown to the civilian citizen. For this reason, they should not be taken as the sole source of information on the basis of which a decision to enter the service is made. They are an excellent way to improve the patriotic education of the young generation. Therefore, it is necessary to promote the possibilities of visiting military formations as much as possible in order to attract many people, especially from schools and youth forums.

Military training classes in schools began after the adoption of the Law on the Reserve in 2013. The order and ways of conducting it were already considered in the analysis of upbringing as an external personal factor. As an upgrade to the lessons in the schools, practical lesson hours or showing formations should be added. This would enable students to experience first-hand the equipment and armament and combine theory and practice.

The credibility of the information offered in each of the mentioned ways is critical to the military recruitment process. Providing only positive information and saving the negative one results in an unrealistic view of the job, which seems to increase the rate of voluntary resignation due to discrepancy with expectations.

By providing up-to-date and timely information about the entire application and selection process, the future military personnel will get the complete picture of how to prepare the necessary documents and the abilities they need for the competition. This will lead to relief for applicants and a decrease in the percentage of voluntary refusals due to the inability to prepare personally and submit documents.

#### **External sources of information**

External sources of information are not under direct organisational control, which is why they are increasingly taken into account by job seekers.

Word-of-mouth sharing is in most cases more highly valued than reviewing organisational features on the organisation's page or through other official sources. Information provided through social contacts (friends, relatives, acquaintances) is perceived as positive and more reliable than the rest, and in addition, the influence of live contact on behaviour is unequivocally more influential. Driven by these findings, military leaders are increasingly using military personnel for word-of-mouth outreach. By sending military personnel to their hometowns to participate in recruitment campaigns for soldiers and candidate cadets, the effect of this approach is quite good. Getting first-hand information through a respectable-looking military person is more powerful than any other ad. When applying this method in combination with an attractive display, the effect of informing is even stronger. This requires using this approach more extensively in order to win the hearts and minds of potential candidates.

Public advertising and publications in public electronic and print media help build the organisational image, but they can also have a negative impact. The media is not under organisational control, so it needs to be approached carefully. The Bulgarian armed forces traditionally present their capabilities and participate in solemn celebrations of holidays with military rituals. In such a case, informing the media in advance of the expected actions by public relations officers is a good approach to minimise incompetent statements and comments.

The presented model for motivating applicants to join the armed forces reflects the factors affecting the process of recruiting military personnel. There are many job seekers, but each of them has individual requirements, abilities and ambitions. The armed forces' activity in the overall process is, through its tools of information and influencing human behaviour, to attract the maximum number of candidates with the necessary abilities to fill the large number of vacancies. The motivation of these candidates needs to be sustained from the time of first contact until entry into military service, with the motivation activity subsequently being taken over by the retention model.

The analysis of the various motivational models showed that the economic condition of the country is directly related to the demand for work. In days of pandemics and crises, armed forces have a real opportunity to attract more applicants, while in days of economic growth, it is very difficult. A nationwide approach is needed to promote the armed forces' reputation as a desirable employer.

#### **CONCLUSIONS**

Motivation is a voluntary mental state of the person, consciously directing individual behaviour to certain actions to achieve set goals. It is intrinsic but influenced by external influences, which must be used by military organisations to attract potential candidates to fill the growing personnel vacuum in the armed forces.

The new realities of the modern world provide immense opportunities to the new 'Z' and 'Alpha' generations; therefore, in order to attract and retain job candidates from these generations in the hectic everyday life, companies and enterprises must be aware of and adapt to the changing workforce needs [6]. This requires the Bulgarian Armed Forces to develop models for attracting and retaining military personnel that are up-to-date with the current reality and the requirements of the labour market and to update them periodically in order to maintain their relevance.

The proposed model for recruiting military personnel does not claim to be exhaustive and comprehensive but takes into account the most important factors shaping the motivational behaviour of job seekers. It should be integrated with the military retention model to maintain the motivation of already recruited candidates.

The positive experience from the considered models and approaches indicates that the motivation of military personnel is not a given. It requires investment in time, resources, and will to be achieved. The key to achieving

and maintaining military motivation is persistence in seeking and refining approaches to managing human behaviour, an activity that must be of paramount importance not only to military commanders and chiefs, but to all government leadership.

#### ACKNOWLEDGMENTS

The publication of the article was financed with funds provided by the National Security and Defence Science Program.

#### REFERENCES

- [1] Grigorov, G., Models and approaches for motivation, recruitment and retention of military personnel in the British armed forces, *International Scientific Journal: Security & Future*, Vol. 4 (2020), Issue 1, pp(s) 27-30, Publisher: SCIENTIFIC TECHNICAL UNION OF MECHANICAL ENGINEERING INDUSTRY-4.0, 2020.
- [2] Григоров, Г., „Модели и подходи за привличане и задържане на военнослужещи в Белгийската армия“, Издание: Сборник доклади от Годишна университетска научна конференция 28-29 май 2020, с. 1423-1434, Издателство: Издателски комплекс на НВУ „Васил Левски“, 2020.
- [3] Григоров, Г., „Модели и подходи за привличане и задържане на военнослужещи в Канадската армия“, Издание: Сборник доклади от Годишна университетска научна конференция 28-29 май 2020, с. 1435-1447, Издателство: Издателски комплекс на НВУ „Васил Левски“, 2020.
- [4] Grigorov, G. Motivation for Choosing and Practicing the Military Profession, *The 26th International Conference The Knowledge-Based Organization 2020*, conference proceedings: 2 , pp. 162 – 169, Nicolae Balcescu Land Forces Academy, Sibiu, Romania, 2020, Available: <http://dx.doi.org/10.2478/kbo-2020-0070>
- [5] Barber, A., *Recruiting employees: Individual and organizational perspectives*. Thousand Oaks, CA: Sage, 1998.
- [6] McCrindle, M. *The ABC of X, Y, Z – Understanding the Global Generations*, UNSW PRESS, 2009, pp. 143 -176
- [7] Grigorov, G., Spiridonov, S., Research on the Motivation for Choosing the Military Career, *The 24th International Conference The Knowledge-Based Organization 2018*, conference proceedings 1 , p. 302 – 307, Nicolae Balcescu Land Forces Academy, Sibiu, Romania, 2018. Available: <http://dx.doi.org/10.1515/kbo-2018-0048>
- [8] Grigorov, G. Lilov, L., Structure of Motivation for Training in Engineering Specialties, *ENTERprise REsearch InNOVation Conference SPLIT, CROATIA, IRENET, Society for Advancing Innovation and Research in Economy*, Vol. 4, No. 1, pp. 388 – 396, Zagreb, Croatia, 2018, Available: <http://dx.doi.org/10.2139/ssrn.3283730>
- [9] Shannon, C., Weaver, W., *The mathematical theory of communication*. Urbana, IL: University of Illinois Press, 1949.
- [10] Behling, O., Labovitz, G., Gainer, M., *College recruiting: A theoretical basis*. Personnel Journal, 47, 1968.
- [11] Collins, C., Stevens, C., Initial organizational images and recruitment: A within-subjects investigation of the factors affecting job choices. Paper presented at the 14th Annual Conference of the Society for Industrial and Organizational Psychology, Atlanta, Georgia, 1999.
- [12] Chapman, D., Uggerslev, K., Carroll, S., Piasentin, K., Jones, D., Applicant attraction to organizations and job choice: A meta-analytical review of the correlates of recruiting outcomes. *Journal of Applied Psychology*, 2005, pp. 928-944.
- [13] *Recruiting and Retention of Military Personnel, Final Report of Research Task Group HFM-107, Research and Technology Organisation (RTO) of NATO*, Oct 2007.
- [14] *Правилник за прилагане на закона за отбраната и въоръжените сили на Република България*, приет с ПМС № 46 от 22 март 2010, обн. ДВ. бр.25 от 30 Март 2010г, изм. и доп. ДВ. бр.76 от 5 Септември 2023г.
- [15] *Закон за резерва на въоръжените сили на Република България*, МО, С., обн., ДВ, бр. 20 от 9.03.2012 г., в сила от 10.06.2012 г., изм. и доп., бр. 109 от 22.12.2020 г., в сила от 22.12.2020 г., чл. 56
- [16] *Наредба за условията и реда за организиране, провеждане и осигуряване обучението на българските граждани за защита на Отечеството*, Приета с ПМС № 66/03.05.2023 г. обн. ДВ. бр.41 от 9 Май 2023г., в сила от учебната 2023/2024 г., чл. 5
- [17] *BULGARIAN ARMED FORCES 2017 - GLORY LASTS FOREVER!* [Online]. Available: <https://www.youtube.com/watch?v=7pJsg8gd-eU&t=4s> [Accessed: Feb. 28, 2024].

# Algorithm for diagnosis of the tank weapon stabilization system "Complex 2E28M" in „Targeting“ mode

**Yordan Hristov**

“Vasil Levski” NMU  
“Logistic and tehnologe” Faculty  
V. Tarnovo, Bulgaria  
danchohr@abv.bg

**Ivan Minevski**

“Vasil Levski” NMU  
“Logistic and tehnologe” Faculty  
V. Tarnovo, Bulgaria  
ivan\_minevski@abv.bg

**Abstract.** The latest trend in the development of combat equipment is the increasing penetration of automated and automatic systems with a variety of purposes. In its bigger part, these systems include electrical machines, electrohydraulic, electronic and gyroscopic units and assemblies. The considerable complexity of the electro-automation of machinery, even with high reliability, leads to an increase in the probability of the occurrence of failures and the need to increase the requirements for the qualification of the engineering staff of the repair staff.

The study of diagnostic and repair issues of electro-automatic systems is based on the knowledge of the faults occurring in the systems in the process of their operation.

The faults of the systems by the cause of occurrence can be divided into: faults resulting from wear and ageing of parts and components; faults resulting from construction errors and from low quality of manufacture; faults resulting from poor quality of servicing and repair; faults resulting from insufficient qualification of the operating personnel.

Failures of systems in terms of their operability can be divided into: failures altering the characteristic of systems and deteriorating the quality of their operation; failures leading immediately to the shutdown of systems; failures directly affecting the quality of operation of systems, their characteristics and subsequently leading to their complete shutdown.

System failures can be divided into: failures requiring repair of the system by replacement of the failed units and assemblies; failures requiring repairs without replacement of the units and assemblies; failures that were being repaired in the process of operation and maintenance of the systems.

Before carrying out an emergency repair of the electro-automation, it is necessary to determine the nature of the fault and to specify as precisely as possible the location of the faulty element or component in the electrical, hydraulic or kinematic circuitry of the electro-automation.

The purpose of the survey is to provide the operating personnel with a sequence of actions which result is in the detection of the fault or qualified personnel to be directed to the most likely faulty component.

An algorithm for diagnostics of the "Complex 2E28M" tank weapon stabilization system in the "Target

Designation" mode is presented. The algorithm is built by using the "Failure Tree" method to determine the state of complex technical systems.

The advantages of the presented method of initial diagnostics are that it is possible for the crew with their own forces and means to detect small failures in the weapon stabilization system. On arrival of the specialised repair bodies, the crew directs them to the most likely cause of failure. In this way, all possible causes of failures in the system are tracked, providing instructions to the operating staff for elimination of the possible failures that have occurred. Using this method the time for product diagnostics is significantly reduced.

**Keywords:** Algorithm, Automatic systems, Diagnostics.

## I. INTRODUCTION

The quality of operation of the automatic systems in the tanks guarantees their high combat efficiency and the fulfillment of their assigned tasks. The accuracy of hitting moving targets to the greatest extent (in purely technical terms) depends on the weapon stabilization system (WST). For this reason, it is a subject of numerous studies. For the needs of the research work and the increase of the efficiency of STV, it is necessary to determine how the individual constructive parameters affect the quality of stabilization.

For indicators of the quality adjustment, the change in the reserve of stability and the speed of action are monitored.

Margin of stability refers to the quality of automatic control systems (CAP) in the non-established modes of operation, being determined by the type of process under some typical setting or disturbing effect.

The stability margin characterizes the tendency of the system to oscillate. The more oscillations the process has, the smaller the margin of stability. Its value is determined by the maximum value of the adjustable quantity referred to its established value after the transition process has taken place [1].

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8199>

© 2024 Yordan Hristov, Ivan Minevski. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

The value of the reregulation depends on the features and requirements of the regulated object (process). It is usually 10% to 30%, but can be outside these limits on some systems. In some cases, reregulation is not allowed at all, which means that oscillations in the system are also inadmissible.

The transient process curve is used to determine the speed of the systems. Fastness indicates the ability of the system to monitor changes in the input (setting) impact. It is defined as the time for which the adjustable quantity reaches a value different from the set one with the advanced set small quantity.

Some other indicators of the transient process curve, such as the time of –growth, are also used to assess the rapidity of action. It is defined as the time necessary for the system to reach for the first time the established value of the adjustable quantity, counted from the moment of application of the setting impact [2].

If there is necessity of deeper analysis the system is required, the identified transmission functions of the electronic amplifier [3], the speed sensor [4], of the angle sensor [5], the hydraulic vertical guidance system [6] can be used, as well as the built and checked for adequacy mathematical model [7] and diagnostic model [8] of the tank armament stabilizer "Complex 2E28M".

To analyze the processes due to the oscillations of the tank body during its movement, the emerging vibrodynamic processes, and their influence on the quality of stabilization of the armament, an analysis of the system using the finite element method is used [9] - [11].

The stabilizer of the tank weapon (STA) "Complex 2E28M" is installed on the T-72 medium tank and its modifications. "Complex 2E28M" is an electro-hydraulic automatic system providing stabilization and guidance of the cannon and the machine gun paired with it in vertical and horizontal planes. It is designed to increase the effectiveness of fire when firing tank weapons while moving. The STA works together with the TPD-2-49 or Quantum TPD-K1 optical sight-rangefinder and the automatic gun loader. Also with the planned thermal imaging observing and measuring devices in the ongoing modernization of the T-72 tank in the Bulgarian Army.

The STA consists of two electro-hydraulic tracking drives: a vertical guidance drive (VD) and a horizontal guidance drive (HD). VD stabilizes the swinging part of the cannon in a vertical plane, and HD stabilizes the turret with the weapon in a horizontal plane.

As a result of the stabilization during the movement of the tank on rugged terrain, the weapon maintains the set position in space, while the tank body fluctuates in the vertical and horizontal planes (VP and HP). At the same time, during the stabilization, the elevation angle of the gun in VP and the azimuth angle in HP can be changed by the rangefinder operator using the control panel located on the sight-rangefinder.

The main modes of operation of the STA are "Semi-automatic", "Automatic" and "Targeting". "Semi-automatic" mode provides unstabilized aiming in HP and manual aiming of weapons in VP. "Automatic" mode provides stabilization and guidance of weapons in VP and HP. "Target Designation" mode provides guidance of weapon to a target selected by the tank commander. In this mode, the commander takes control of the HP from the gunner and directs the cupola at maximum speed to a

target of his choice. During targeting, the gunner receives a light indication. Targeting can be used during STA operation in "Automatic" and "Semi-automatic" modes.

In order to quickly and accurately identify the defective elements and units in the automatic system, it is necessary to create an appropriate action algorithm. The application of this algorithm will greatly facilitate service personnel in detecting the causes of system failure.

## II. MATERIALS AND METHODS

In its composition, "Complex 2E28M" includes a number of electrical machines, electrohydraulic, electronic and gyroscopic units and assemblies. The significant complication of STA, even with high reliability, leads to an increase in the probability of the occurrence of failures and the need to increase the requirements for the qualification of the engineering staff of the staff. The study of questions about the diagnosis and repair of electro-automatic systems is based on the implementation of operational methods and the knowledge of malfunctions that occurred in the systems during their operation.

Before carrying out an emergency repair of the electrical automation, it is necessary to determine the nature of the malfunction and specify as precisely as possible the location of the damaged (obsolete, worn) element or detail in the electrical, hydraulic or kinematic scheme of the electrical automation.

In the event of a loss of operability of the electrical automation or a separate system of its with obvious external damage the following is carried out:

- Detailed external examination in which additional and other obvious malfunctions could be detected;
- Removal of all external damages for which dismantling of main blocks is required.
- Checking off the functionality of the electro-automatics, which gives opportunity to detect any internal damage before proceeding to dismantle main blocks;
- Dismantling of the main blocks in which there is external or internal damage;
- Checking the dismantled blocks using special equipment. This check is carried out in the presence of specialized diagnostic equipment;
- Installation of the blocks;
- Checking the operability of electro-automatic in all modes of operation.
- Targeting mode is activated in the following sequence:
  - Turns on STA in "Semi-automatic" or "Automatic" mode;
  - The commander's cupola is locked. If it is locked, Target mode does not work;
  - Aim the commander's sighting device at the target and hold it there;
  - The targeting buttons located on the left and right grips of the commander's observation instrument are pressed. At the same time, the control of the cupola from the gunner is transferred to the commander, and the "Commander" signal lamp lights up on the signal board of the sight-rangefinder. When buttons are pressed, the turret rotates at maximum transfer speed to the target. Upon reaching the direction of the target, the turret stops its movement;

➤ After the cupola stops, the buttons are released. This extinguishes the "Commander" signal light and the control of the guidance of the cupola is transferred to the gunner. It carries out the precise guidance of the weapon to the target.

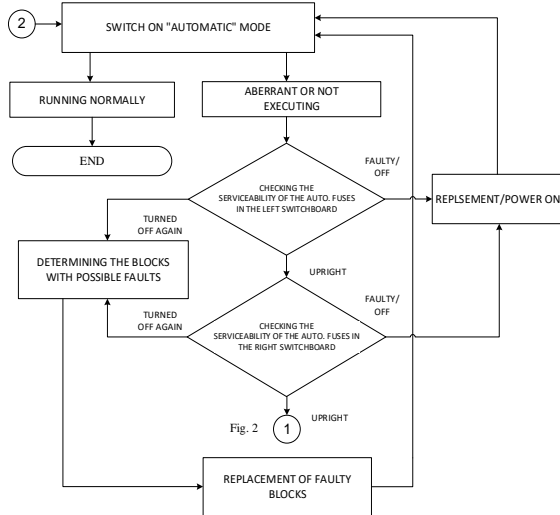


Fig. 1. Algorithm /first part/ for diagnosis of STA in "Targeting" mode.

### III. RESULTS AND DISCUSSION

To detect the block in which a failure occurred, it is necessary to apply the algorithm shown in figures 1, 2, 3 and 4 for diagnostics of STA in the "Targeting" mode, based on the algorithm for diagnostics in the "Auto" mode [12].

For this purpose, the activities of preparing the system for inclusion are carried out, then in strict sequence, the STA is turned on in "Automatic" mode.

In the sequence of the algorithm, the elements for control in case of failure or atypical operation of the system are specified.

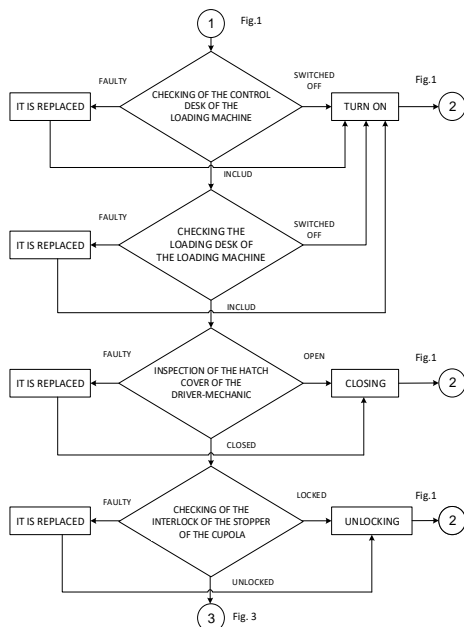


Fig. 2. Algorithm /second part/ for diagnosis of STA in "Targeting" mode.

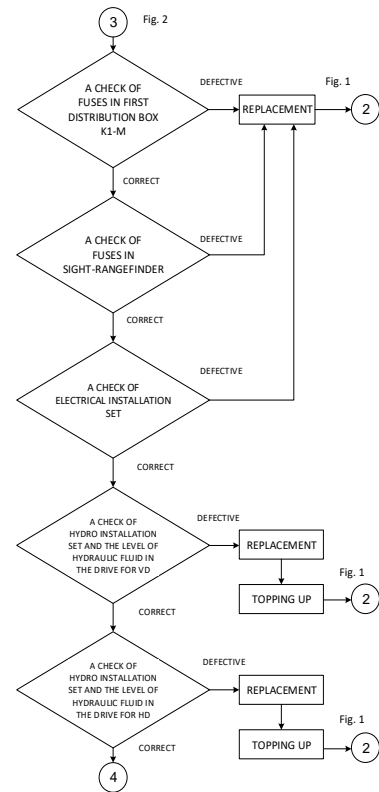


Fig. 3. Algorithm /third part/ for diagnosis of STA in "Targeting" mode.

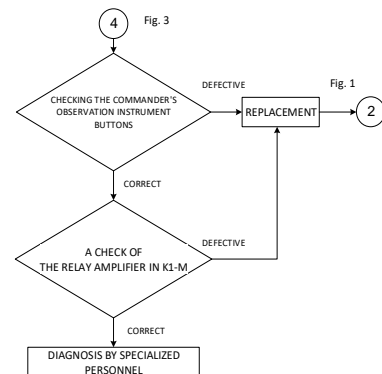


Fig. 4. Algorithm /fourth part/ for diagnosis of STA in "Targeting" mode.

During switching on of the STA, in the absence of specialized equipment, the fault is localized by the method of replacement: one by one, the blocks identified as possibly faulty are dismantled, in their place, serviceable blocks from the stock are installed and the operability of the electrical automation after each successive shift is checked. Restoration of operability is an indication that the replaced unit is damaged. If operability is not restored, another unit or several units are damaged at the same time. In such a case, complete and accurate conviction of the location of the damage can be achieved by checking the operability of the STA by successively changing all possible combinations of the recorded blocks.

If specialized equipment is available all blocks that are identified as possibly faulty are checked. If they are found to be working, the remaining blocks and all connecting wires and plug joints are checked. Damaged blocks are dismantled and replaced with new or repaired ones.

No other literature is available on this problem for this particular system.

#### CONCLUSIONS

1. Adhering to the proposed algorithm, it is quite possible with the forces and means of the crew to discover the reason for the malfunction of the weapon stabilization system and to locate the faulty unit, without using specialized diagnostic equipment and highly qualified engineering and technical staff.

2. The widespread introduction of automatic systems in combat equipment, on the one hand, leads to an increase in its efficiency and convenience in operation, but on the other hand, the probability of failures due to which it cannot fulfil its functional purposes increases.

3. The developed diagnostic algorithm will increase the efficiency of the technical staff during the repair and restoration activities when eliminating the troubleshooting of the automatic weapons control systems.

#### 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] Y. Hristov, "Influence of the torsional stiffness of the angular velocity sensor on the quality of stabilization of tank armament", Military Scientific Forum 2007 with international participation V. Levski National University, 2008, pp. 319-326, ISSN 1313 -0390.
- [2] Y. Hristov, "Influence of the transmission coefficient of the angular deviation sensor on the quality of stabilization of the tank armament", The Annual University Scientific Conference of the Vasil Levski National University September 30-October 1, 2010, 2011, ISSN 1314-1937.

- [3] Y. Hristov, "Identification of the transmission coefficient of the electronic amplifier from the weapon stabilization system "Complex 2E28M", Scientific works - Vasil Levski National Military University, 2003, pp. 566-572, ISSN 1313-8553.
- [4] Y. Hristov, "Identification of the transmission function of the speed sensor from the armament stabilization system "Complex 2E28M", Scientific works - Vasil Levski National Military University, 2003, pp. 562-565, ISSN 1313-8553.
- [5] Y. Hristov, I. Lilov, S. Stefanov and L. Lalev, "Identification of the transmission coefficient of the angle sensor from the weapon stabilization system "Complex 2E28M", Days of Science `2003, Union of Scientists in Bulgaria Branch Veliko Tarnovo, 2003, pp. 356-359, ISBN 954-775-259-6.
- [6] Y. Hristov, S. Stefanov and I. Lilov, "Identification of the parameters of the transmission function of the hydraulic system for vertical guidance of "Complex 2E28M", Military Scientific Forum 2000, Union of Scientists in Bulgaria branch V. Tarnovo, 2000, with 505-510, ISSN 0861-0312.
- [7] Y. Hristov, I. Minevski and T. Yotkov, "Mathematical model of the system for tank armament stabilization "Complex 2E28M", Annual University Scientific Conference of NMU "V. Levski" - June 27-28, 2019, pp. 164-173 , ISSN 1314-1939 ISSN 2367-7481.
- [8] Y. Hristov, I. Minevski and T. Yotkov, "Diagnostic model of the system for tank armament stabilization "Complex 2E28M", VII International scientific and technical conference engineering. Technologies. Education. Security. Veliko Tarnovo, Bulgaria 29 May - 01 June 2019 , p. 1797-1803, ISSN 2535-0315 (Print) ISSN 2535-0323 (Online).
- [9] T. Yotkov, "Frequency analysis of the system body of a transport machine - DVG by the method of finite elements", Magazine. "Mechanics of Machines" No. 28, book 4, pp. 106-109, Publishing House of TU Varna, 1999, ISSN 0861-9727.
- [10] T. Yotkov, "Finite element model of an armored personnel carrier", Collection "Military Scientific Forum", c. 208-214, IC of NMU "V. Levski", September, VT, 2000, ISSN 0861-0312.
- [11] S. Spiridonov, S. Stefanov and T. Yotkov, "Study of the vibrodynamic processes occurring in the suspension of a light armored car, when firing with mounted weapons from a location", International scientific and technical conference "Technique. Technologies. Education. Security." 14 Veliko Tarnovo 29.05. - 30.05.2014, pages: 7, ISSN 1314-1937 - 2014
- [12] Y. Hristov and I. Minevski, "Algorithm for diagnostics of the tank armament stabilization system "Complex 2E28M" in the "Automatic" mode", The annual university scientific conference of NMU "V. Levski" with international participation - June 8-9 2023 pp. 1185-1190 ISSN 2367-7481.



# Green and Social Innovations in Providing Effective Prevention and Security for Active Ageing

**Maria Ilcheva**

Department of National Security  
St. Cyril and St. Methodius  
University of Veliko Tarnovo  
Veliko Tarnovo, Bulgaria  
[mkilcheva@abv.bg](mailto:mkilcheva@abv.bg)

**Abstract.** The ageing population will soon become one of the most demanding Big Societal Challenges that the world will face. In European union the percentage of the population over 60 years old is expected to increase from 20% to 33% between 2015 and 2050. The report reviews and analyses the role and potential of green and social innovations to foster the active ageing through complex research methods such as an in-depth study of main effects and added value of good practices that demonstrate the contribution of green and social innovations. The main objective of the paper is to analyze the main factors related with social and green innovations that foster healthy ageing and effective prevention and security of elderly people at a reasonable cost. The main conclusion of the research is that it demonstrates the potential of social and green innovation to improve the quality of life and personal security of old people while taking into account the new concepts and instruments related with the elements of Active Ageing Index.

**Keywords:** ageing population, prevention, social security

## I. INTRODUCTION

All countries in Europe are facing a dramatic societal challenge with the ageing population. By 2024, it is estimated that the population of individuals aged over 65 years will outnumber those under the age of 15. By the end of the current decade, the number of people aged 60 years and older will be 34% higher, increasing from 1 billion in 2019 to 1.4 billion. By 2050, the global population of older people will have more than doubled, to 2.1 billion [1]. This trend means new social, economic and health challenges, which demand a focus on healthy ageing to mitigate the impact of an ageing population. The current report is looking into the potential of social and green innovations that can mitigate the consequences for health and wellbeing of old people and improve their social security.

The purpose of the report is to review and analyze the role and potential of green and social innovations to foster the active ageing through complex research methods such as an in-depth study of main effects and added value of good practices that demonstrate the contribution of green and social innovations. An additional task of the current research is to analyze the main factors related with social and green innovations that foster healthy ageing and effective prevention and security of elderly people. Key methodological approach is the critical study of green and social innovations, their contribution to the assessment of Active ageing index and the applied contribution to better quality of life and improved security for elderly people. In order to introduce the conceptual framework the active ageing is defined as “helping people stay in charge of their own lives for as long as possible as they age and, where possible, to contribute to the economy and society”. The author explores an interdependency between the level of wellbeing as a factor for active ageing and the provision of social and health services, which are driven by social and green innovations. Furthermore, the article explores the areas in which social and green innovations are appearing in order to contribute to active, healthy and secure life of elderly people.

The phenomenon of ageing population. The aging process refers to the biological changes that occur over time, resulting in a gradual loss of physiological integrity, diminished function, and increased mortality risk [2]. Aging involves the deterioration of bodily functions and a decline in physical and mental capacity, primarily driven by cellular damage [2]. While aging is a primary risk factor for various diseases, it is important to recognize that aging itself is not a disease but a natural phenomenon. World Health Organization identifies active ageing as a “process of optimizing opportunities for health, participation and security, in order to enhance quality of life as people age” [3]. Active ageing is defined by the

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8205>

© 2024 Maria Ilcheva. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

European Commission as “helping people stay in charge of their own lives for as long as possible as they age and, where possible, to contribute to the economy and society” [4].

## II. ACTIVE AGEING INDEX

In this study, environmental and social innovations are associated with the availability of social and environmental investments aimed at achieving a positive effect on people and their security and wellbeing. At the same time, environmental and social governance is a key social security variable whose dynamics influence security factors. There is a direct dependence on social security, which is linked to increased investment in social infrastructure in order to strengthen the social protection systems that are crucial for the fight against poverty and inequalities.

In recent years, the trends in Europe have been quite negative, widening the gap between people's needs and the actual investments mobilized for social infrastructure, which are key determinants of social security. A number of studies by the World Health Organization show that public investment in social infrastructure is 20% lower than a decade ago, which means that services such as social assistance, health and social protection have reduced their standards and cannot meet existing needs.

The Active Ageing Index is a tool to measure the untapped potential of older people for active and healthy ageing across countries. It measures the level to which older people live independent lives, participate in paid employment and social activities, and their capacity to age actively [5].

Active Ageing Index (AAI) was developed and launched in 2012, in collaboration with the European Centre for Social Welfare Policy and Research in Vienna and with the support of the multi-stakeholder Expert group on AAI. It consists of four main areas as shown below in Fig. 1.:



Fig. 1. Components of Active Ageing Index  
(Source: Leaflet on Active ageing index,  
<https://unece.org/population/active-ageing-index>)

The Active ageing index includes 22 indicators grouped into four domains - employment; participation in society; independent, healthy and secure living; and, the capacity and enabling environment for active ageing. The third domain for independent, healthy and secure living presents more examples of social and green innovation related with access to health services, physical safety and lifelong learning. Therefore, the fourth domain related with capacity and enabling environment for active ageing is focusing on green spaces and environment that contributes to physical, mental and social health of elderly people, and the maintenance of ecosystem services and biodiversity. Bulgaria is occupying a lower

place in the index ranked with an overall score of 31.8 compared to the average score for the European Union of 35,7.

## III. SOCIAL AND GREEN INNOVATIONS FOR ACTIVE AGEING

The concept of social and green innovations does not have a single definition due to the multifaceted character of social challenges that are driving the social sector and the green transition. The numerous social risks that are accompanying the old population have a direct impact on their health, wellbeing and quality of life. The idea that social innovation is an effective way for dealing with societal challenges is manifested in policy discourses across the EU. Practitioners, scientific observers and other parties with interests in social innovation have reasons to believe that it can contribute to social transformation, and to consider the attendant practical challenges of such transformative social innovation.

Researchers and organizations dealing with this topic mainly use the general definition, which assumes that social innovation is an action based on both social ends and social means, which include new ideas (products, services, and models) that meet social needs (more effectively than alternatives) and create new social relationships or collaborations [6].

Green and social innovation can be reviewed in three main aspects related with prevention and support of ageing population such as:

- Innovations in service delivery – mobile and integrated social services, telemedicine for health diagnostics and access to health support;
- Innovations in green infrastructure for active ageing
- Security innovations for elderly people

### A. *Innovations in service delivery*

Digitalization and information technology are perceived as a tool that optimizes the logistics chain in the provision of social services. At the same time, they are a major factor in moving towards environmental practices, especially when it comes to providing access to services to people in remote and sparsely populated areas. An example of the use of information technologies for the provision of health and social services is a social innovation for the implementation of telemedicine of the Municipality of Burgas.

The social innovation that is gaining popularity among Bulgarian municipalities is offering access to health services through information technologies, or so-called telemedicine. Burgas Municipality is one of the pioneers in Bulgaria in providing remote health services through telemedicine to hard-to-move and lonely elderly citizens who are users of social institutions in the city. The motives for this initiative are the increasing number of disabled and lonely elderly people using various social services in the municipality of Burgas, their need for consultations with specialist doctors and difficult access

to medical care due to their health condition or pandemic restrictions.

On the other hand, telemedicine will allow the necessary access to special care to be provided, even if the specialist concerned is located at a great distance. It offers a convenient way of communication between doctor and patient, eliminating the need for a physical visit to the doctor's office, especially in the period of influenza epidemics, bad weather conditions or difficult mobility of service users. Users of social services usually need help in adjusting drug doses, determining diet and physical activity, prescribing prescriptions for medications that have already been prescribed to them once. Therefore, telemedicine is a good solution for tracking patients with chronic diseases such as diabetes, high cholesterol or arterial hypertension.

With remote access to medical equipment, doctors can monitor and control their old patients and respond to their needs. The advantages of applying the social innovation are access to consultation with a specialist doctor beyond the limitations of specific medical fields, shortening the time between the occurrence of a health problem and primary consultation, improving the quality of health services, especially when tracking patients with chronic diseases, security for patients in epidemic situations, etc.

Information technologies are gaining popularity in social logistics, especially when they provide long-distance health care, which means that people in remote areas with limited access to healthcare can get the medical care they need. This saves time and resources for both doctors and patients and is a favorable opportunity to improve the quality and efficiency of social and health services. Innovative e-Health solutions can support disease prevention and promote healthy lifestyles, lead to improvements in citizens' quality of life and enable more effective ways of organising and delivering health services and care.

#### *B. Green spaces for active ageing*

As a complex green and social innovation, we can point out the design of friendly infrastructure for active walking. Walking for an average of 30 minutes a day can lower the risk of heart disease, stroke, and diabetes by 30% to 40%. Walking is associated with increased social interaction, the development of social capital and increased safety [7].

Green urban environment is widely accepted as a stress reduction factor. It is generally agreed that long term exposure to urban stressors such as noise, crowding and fear of crime without possibilities for restoration from stress, can affect mental health and increase the risk of depression, anxiety and fatigue syndromes [8]. Researchers have also demonstrated that increased access to green space may be linked to reductions in neighbourhood crime, violence, and aggression, which is a key factor for the security of old, people [9]. Access to green environment can also enhance social cohesion and reduce social risks for elderly people.

Design and delivery of open spaces that promote the health and wellbeing of people and the natural

environment is a key challenge for health and urban planning in rapidly growing cities. There is growing recognition of the need for higher-density more compact urban form to accommodate the growing urban populations.

Neighbourhood connection, social capital and a strong sense of community are important because these have all been shown to be associated with improved wellbeing, increased feelings of safety and security, participation in community affairs and civic responsibility. Moreover, access to urban green space has also been linked to positive indicators of functioning societies, such as reduced fear and reduced levels of crime [10].

#### *C. Security innovations for elderly people*

A number of researchers point out that one of the most important conditions for the protection of mental and physical health is the guarantee of social security, which is directly dependent on the presence of social sensitivity in society [11, 12]. According to Yonchev, the security of communities determines the security of the individuals involved. In confirmation of this theory is the notion that any change in the environment has an impact on security by implying some response and can be understood as a reaction to an emerging and conscious challenge. The personal security environment can be seen as a state of absent risks and clearly defined and controlled threats to the individual and his physical and mental health, as well as his lifestyle [12].

Despite the availability of a number of technologies and innovations in social logistics to improve personal security, large groups of society remain quite vulnerable. Such a vulnerable group in terms of security are the elderly in urban environments. The proportion of people aged 65 and over who feel safe when walking alone in their neighbourhood measures the concept of 'fear of crime'. According to the data, 21.4% of older people (aged 65 and over) feel insecure walking alone in their neighbourhood (locality), almost twice the proportion of people in any other age group [13]. In addition, according to Eurostat, in 2019 the share of people in Bulgaria reporting crime, violence or vandalism in their neighborhood was the highest in the EU – 20.2%.

#### **IV. NEW CHALLENGES FOR THE FUTURE**

Over the last 150 years, life expectancy has risen by 50 years, and over the last half century, alone it has increased by three years every decade [14]. Growing challenges for the future are to provide effective prevention and support for ageing population at a reasonable cost. Healthy ageing facilitated by green and social innovations can be a reality for all. This will require a shift in focus from considering healthy ageing as the absence of disease to fostering the functional ability that enables older people to be and to do what they value. Actions to improve healthy ageing will be needed at multiple levels and in multiple sectors to prevent disease, promote health, maintain intrinsic capacity and enable functional ability [15].

A recent OECD study on social innovation confirms that improved access to integrated services such as health, childcare, housing and others for the elderly and people with disabilities can contribute to a significant reduction in inequality in society, reduce the level of poverty across different social segments, and thus increase social security [16]. The main directions in which the development of social innovations should be considered is to increase the opportunities for active ageing and improved social security for all generations.

At the same time, we are witnessing the growing role of digital technologies that promote social progress, facilitate innovation, increase security, while helping to improve personal security. More and more of the so-called critical activities, with most economic and social activities being entirely dependent on digital technologies. These activities include the health, safety and security of citizens, the effective functioning of basic services, as well as economic and social prosperity more broadly. Examples of such critical activities include a range of public services such as water and energy supply, health and social care provision, telecommunications, transport and urban services.

#### CONCLUSION

The main aim of this article was to provide a comprehensive overview of the development of social and green innovations and to emphasize the importance of new research in the field to promote active aging. With the continually growing older adult population, efforts should be directed towards exploration and integration of smart and ecological solutions that can positively influence physical and psychological wellbeing.

According to the World Health Organization, an age-friendly environment aims to promote active and healthy ageing by optimizing health, fostering inclusion and ensuring well-being in old age [17]. It adapts the physical and social environment to the needs of older people with different abilities. While the supportive physical environment focuses on components such as external environment, transport and mobility, and housing, the social dimensions of an age-friendly environment encompass areas such as social participation, social inclusion and non-discrimination, and civic engagement and employment. In general, the more accessible and age-friendly an environment is, the more active older people can be.

Furthermore, the current research demonstrates the potential of social and green innovation to improve the quality of life and personal security of old people while defining the key role of information technologies. The authors has outlined three areas related with innovations in social services, innovations in green infrastructure for active ageing and security innovations for elderly people.

#### REFERENCES

- [1] United Nations, "UN Decade of healthy ageing: Plan of action 2021 – 2030", [Online] available: <https://cdn.who.int/media/docs/default-source/decade-of-healthy-ageing/decade-proposal-final-apr2020-en.pdf> [Accessed Feb. 10, 2024].
- [2] López-Otín, C.; Blasco, M.A.; Partridge, L.; Serrano, M.; Kroemer, G. "The Hallmarks of Aging" 2013, *Cell*. 2013 June 6; 153(6): 1194–1217. Available: PMC PubMed Central, <https://pubmed.ncbi.nlm.nih.gov/23746838/> <https://pubmed.ncbi.nlm.nih.gov/23746838> [Accessed Feb. 10, 2024], doi: 10.1016/j.cell.2013.05.039
- [3] World Health Organization, "World Report on Ageing and Health"; World Health Organization: Geneva, Switzerland, 2015, available: <https://www.who.int/publications/i/item/9789241565042> [Accessed Feb. 9, 2024].
- [4] Eurofound (2018), "Active ageing", *European Industrial Relations Dictionary*, Dublin, [Online]. Available: <https://www.eurofound.europa.eu/en/european-industrial-relations-dictionary/active-ageing> [Accessed Feb. 9, 2024].
- [5] United Nations Economic Commission for Europe, "2018 Active Ageing Index analytical report", United nations, Geneva 2019, [Online]. Available <https://unece.org/population/publications/active-ageing-index-analytical-report> [Accessed Feb. 9, 2024].
- [6] R. Murray, J. Caulier-Grice and G. Mulgan, "The Open Book of Social Innovation", London: NESTA, 2010. [E-book] Available: <https://youngfoundation.org/wp-content/uploads/2012/10/The-Open-Book-of-Social-Innovation.pdf>
- [7] D. Sinnett, K. Williams, K. Chatterjee, N. Cavill "Making the case for investment in the walking and cycling environment" *Living Streets*, 2011. [Online]. Available: Semantic scholar, <https://www.semanticscholar.org/paper/Making-the-case-for-investment-in-the-walking-A-of-Sinnett-Williams/6284e286cbf7bbf40a77a845758200193a7f0bda>, [Accessed Feb. 10, 2024].
- [8] M. F. Marin, et al. "Chronic stress, cognitive functioning and mental health." *Neurobiology Learning Memory* Vol. 96 (4): p. 583-595, 2011, Available: Science Direct, <https://www.sciencedirect.com/science/article/abs/pii/S1074742711000517>, [Accessed Feb. 10, 2024] <https://doi.org/10.1016/j.nlm.2011.02.016>
- [9] Davern, M., Farrar, A., Kendal, D. & Giles-Corti, B. "Quality Green Public Open Space Supporting Health, Wellbeing and Biodiversity": A Literature Review. Report prepared for the Heart Foundation, 2016, University of Melbourne: Victoria. [Online]. Available: Nature for Health and Wellbeing, [https://issuu.com/royalbotanicgardensvictoria/docs/rbg260\\_nature\\_for\\_health\\_and\\_wellbeing\\_report\\_-\\_fa](https://issuu.com/royalbotanicgardensvictoria/docs/rbg260_nature_for_health_and_wellbeing_report_-_fa) [Accessed Feb. 10, 2024].
- [10] F. E. Kuo and W. C. Sullivan "Environment and crime in the inner city does vegetation reduce crime?" *Environment and Behavior* Vol. 33, no 3, p. 343-367 (2001). Available: Sage Journals, <https://journals.sagepub.com> [Accessed Feb. 10, 2024] , <https://doi.org/10.1177/0013916501333002>
- [11] V. Buzov, *Decisions and security*, University print house "St. Cyril and St. Methodius", Veliko Tarnovo, 2015 pp. 58-60
- [12] D. Yonchev, "Levels of security", *New Bulgarian University*, Sofia, 2008, pp. 28-35
- [13] European Union, "Key indicators on social inclusion and fundamental rights in Bulgaria", Agency for Fundamental Rights (FRA), Thematic report on the elderly, 2021
- [14] V. Mioria, D. Russo, L. Ferrucci "Supporting Active Aging Through A Home Automation Infrastructure for Social Internet of Things", *Volume 3, Issue 4*, p. 173-186 (2018). Available: *Advances in science*, <https://www.astesj.com/v03/i04/p15/> [Accessed Feb. 10, 2024], doi: 10.25046/aj030415
- [15] United Nations, "Progress report on the United Nations decade of healthy ageing 2021 – 2023", *World Health Organization*, November 2023. [Online]. Available: <https://www.who.int/publications/i/item/9789240079694> [Accessed Feb. 10, 2024].
- [16] OECD "Social economy and the Covid-19 crises; current and future roles", OECD, July 2020, [Online]. Available: <https://www.oecd.org/coronavirus/policy-responses/social-economy-and-the-covid-19-crisis-current-and-future-roles-f904b89f/> [Accessed Feb. 10, 2024].
- [17] World Health Organization "Health Promotion Glossary of Terms" *World Health Organization*: Geneva, Switzerland, December 2021, [Online]. Available: <https://www.who.int/publications/i/item/9789240038349>, [Accessed Feb. 10, 2024].

# *Indicators of military capabilities of enemy sabotage-reconnaissance groups and their modelling*

**Nikolay Iliev**

Security and Defense Faculty  
Vasil Levski National Military  
University  
Veliko Tarnovo, Republic of  
Bulgaria  
ntiliev@nvu.bg

**Abstract.** *In the process of modelling combat operations and to organize the fight against sabotage-intelligence groups, estimates of their combat capability indicators have been derived and suggested.*

**Keywords:** *military capability, modelling, sabotage-reconnaissance groups.*

## I. INTRODUCTION

The problem of organizing and leading combat against sabotage-intelligence groups (SIGs) is especially relevant in the case of making informed decisions by commanders at different levels. Commanders and staffs in the maintenance and supply subunits and units have varying degrees of training in this regard. It is this current study that looks at the possibility of organizing the fight against enemy sabotage-intelligence groups in army settings and modelling the combat activities in which they participate by offering estimates of the combat capabilities of the SIGs. In the absence of full-time subunits to face and counteract the first blow of the enemy SIGs and sabotage-intelligence subunits (SISs), significant help may be provided by specialized software products that ensure proper organization, planning, and combat against sabotage-intelligence formations (SIFs) of the probable adversary. This would help them to uncover basic interconnections and ease them in revealing the center of gravity and critical points [1].

## II. MATERIALS AND METHODS

In the article, the system approach is used, as the most appropriate way to study interconnected and related activities, to compare them, as a result of which to draw the appropriate conclusions about their development, realized through:

Methods of theoretical research used in the process of researching sources of information for evaluation and content, comparing activities and reporting on previous experience: theoretical analysis, comparison and synthesis; logical modeling.

Military science analysis was also used to examine trends in the development of concepts for the use, preparation and operation of small units.

It should be noted that a significant part of the document has been omitted and this should be known by the esteemed readers.

## III. RESULTS AND DISCUSSION

The environment in which the units operate increases its components as technology develops and new tactics are applied. This process increases the levels of uncertainty that military commanders face and creates the need for greater adaptability to the operational environment [2]. There will always be a degree of uncertainty that is difficult to quantify, which causes the first problem in the development of such software products – the modelling of combat operations in order to quantify the combat capabilities of the SIGs and to predict the results of their actions [3].

In popular mathematical models of combat operations, in addition to global calculations of the ratio between forces and means taking part in the combat, complex quantitative assessments of systems with which units (typically battalions) and formations are equipped are also performed

When modelling the combat capabilities of the forces and the means of combat (on a battalion level or higher) and evaluating the quantitative-qualitative ratios of both

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8241>

© 2024 Nikolay Iliev. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

parties, it is necessary to analyse performance criteria, such as:

- time for task completion;
- the likelihood of hitting the sites with counteraction;
- proportionality ratios and combat capabilities of the groups;
- the amount of losses incurred and inflicted, etc.

In determining the combat potentials that are the basis for making comparative assessments, they are almost not taken into account, because the combat capabilities of the SIFs are “extremely small”, formed on the basis of the regular subunits of the special forces.

Well-known mathematical models of combat operations provide a comprehensive quantitative assessment of the weapon systems in the units (most often a battalion) and formations [4], determine the combat capabilities of forces and means (battalion and higher), and optimize performance criteria.

An analysis of the SIG’s actions shows that non-fire capabilities characterize the quality of the intelligence subunits’ weapons. For this purpose, it is important to determine values that depend on the time elapsed since the start of combat actions. The following are offered as:

- number of surviving personnel;
- the value of material costs for intelligence;
- the cost of a single reconnaissance site;
- mathematical expectations related to the area of the reconnaissance site and the part of the objects found, etc.

In his work [5], S. Stanev analyses subunits’ combat capability, taking into account the enemy total losses caused by all the fighters and the teams belonging to those units. The value of total losses in equal conditions depends on the combat capabilities of the subunit and the level of manifested commanding skills. Here is an interesting link that is made between combat capability as a function of the combat capabilities of the subunits.

The purpose of modelling combat capability and SIG’s combat capabilities and determining their indicators is twofold: on the one hand, a separate model must be drawn up to predict the actions of the SIG, and on the other, to define quantitative summarised indicators from the SIG model to participate in a common military model of combat. These indicators will be the link between the two models, and will be able to satisfy the input data requirements for the existing common military models set out in formulas (1) and (2).

Combat capabilities of the SIG depend on:

- personnel numbers;
- the level of combat training;
- physical training;
- moral and mental condition;

- the amount of weapons and their fire capabilities;
- logistics;
- command staff training;
- ways to transfer to the rear of the enemy;
- the depth of their combat tasks;
- manoeuvrability and their pace of movement;
- the time to prepare for action;
- the ability to survive in extreme conditions, the strength and nature of the opponent's counteraction, regional terrain and geographical features;
- meteorological conditions, etc.

It is assumed that the available combat capability (CC) of the sabotage-intelligence group will be quantified through losses  $M_{sum}$ , such as:

$$M_{sum} = f(CC_{sum}) \quad (1)$$

$$CC_{sum} = f(Kct(exs), Kca(exs), CC_{weap}(exs), CC_{pers}(exs), CC_{inf}(exs)) \quad (2)$$

where:

$Kct(exs)$  is a quotient of the combat task;

$Kca(exs)$  – quotient of the commander’s actions;

$CC_{weap}(exs)$  – combat capabilities (CC) of weapons;

$CC_{pers}(exs)$  – CC of the SIG, depending on the personnel training;

$CC_{inf}(exs)$  – combat capabilities of the SIG, determining its ability to reconnoitre and transmit information that causes loss to the enemy.

The index (exs) reflects the fact that the given indicator will be modelled and determined through the Expert System (ExS) apparatus, due to the inability to obtain its exact values through standard calculations at the required time, or even to obtain information about them.

The combat capabilities of weapons ( $CC_{weap}$ ) are determined by: the combat capabilities of individual and collective weapons ( $CC_{weap ind}$ ), the presence of explosives in the SIG, as well as devices for carrying out sabotage actions ( $CC_{weap sab}$ ), use of other combat and special equipment ( $CC_{weap spec}$ ).

Combat capabilities of individual and collective weapons of the SIG are manifested mainly in two cases: when there is a need for fire support of the other subgroups participating in the action, or when the whole group has to lead a defensive battle.

Then the main indicators of ( $CC_{weap}$ ) are:

- nomenclature of small arms and heavy weapons (including anti-tank weapons, heavy machine guns and mortars);
- the amount of ammunition for each of them;
- firepower of the salvo of the SIG;
- probability of being struck.

(CCweap sab) will be measured by the potential losses of the enemy after the execution of the sabotage actions equated to the combat potential of the battalion.

The combat capabilities of the group's personnel (CCpers) will be determined by the losses inflicted on the enemy because of the individual capabilities of the SIG fighters which depend mainly on their training. Here, the indicators that influence the result are:

- personnel numbers in the group;
- depth of combat tasks;
- manoeuvrability and pace of movement;
- ways of transfer;
- time for planning and preparation of actions;
- the level of combat training, physical training, and moral and mental status of the group.

The last three indicators depend on the following factors:

- group integration taking into account: assembly and cohesion, psychological compatibility, pride in belonging to the group, attitude to the nation and the armed forces, correctness in relations, common ritual available, presence of kinship and other relationships;
- leadership taking into account: the need for coercion, the interests of the group, the individual interests of each fighter, the degree of need for leadership;
- physical fitness taking into account: the age of the soldiers, their training (complex factor), the dependence of the fighters on food and water, their ability to survive in extreme conditions, stress resistance, mobility, etc.;
- training taking into account: the combat experience of the group, sustainability of knowledge and skills (a complex factor accounting for the difference in the training of an SIG fighter compared to the fighter from a conventional infantry unit), the degree of automaticity in the operation with weapons and special equipment, knowledge of the tactics of action of the SIF and the enemy, individual medical training;
- personal qualities that take into account: the fighter's patriotism and fanaticism, his religiosity and hope for a favourable outcome of the fight, a sense of his need for the group, independence, firmness and readiness for sacrifice, courage, etc.

The groups of factors listed above strongly influence the personnel combat capabilities, but they can only be accurately quantified as a result of the work of an expert subsystem.

It is possible to use a second-generation ExS [6] based on a model and the heuristic knowledge of experts [7] to

solve modelling tasks for combat capabilities of military groups. Taking into account the factors affecting combat capability, their numbers and functional relationships, though with some weaknesses, this would improve knowledge [8] about the real truth of their combat capabilities.

## CONCLUSIONS

1. As a summary quantitative indicator of the personnel combat capabilities, it is proposed to use the time indicator for the combat task  $tct(exs)$ , as well as a function of the above indicators and factors.

2. The following key indicators are offered to determine the combat capabilities  $CC(exc)$ :

- mathematical expectation of the intelligence area and of the part with open sites in the area;
- working capacity and operational range of available communication equipment;
- value of material costs for intelligence and material resources spent.

3. Modelling losses caused by the combat capabilities of the SIG refer to the so-called available combat ability of the group. For it to be real, the  $Kct(exs)$  must be determined using the ExS, taking into account the following conditions:

- whether the combat capability in question applies to tasks specific to the group, each of which is addressed in the typical or not variants and conditions (day, night, offensive, defence, etc.);
- the maximum combat pressure in solving these tasks, with a length typical for each of them, for which all systems must be activated;
- the enemy's actions.

4. The presented study examines the possibility of organizing the fight against enemy subversive-reconnaissance groups in an army setting and modeling the combat actions in which they participate, offering estimates of the combat capabilities of SIGs. In the absence of regular units to meet and counter the first strike of enemy SIGs and subversive-intelligence units (SIS), significant help can be provided by specialized software products that ensure proper organization, planning and combating subversive-intelligence formations (SIF) of the likely adversary.

## REFERENCES

- [1] R. Marinov, S. Stoykov, P. Marinov. Urbanized territories non-existing part of crisis response operations, 2019 International Conference on Creative Business for Smart and Sustainable Growth, CreBUS 2019; Sandanski; Bulgaria; 18 March 2019 through 21 March 2019; Category number CFP19U17-ART; Code 152084, ISBN: 978-172813467-3, Source Type: Conference Proceeding, Original language: English, DOI: 10.1109/CREBUS.2019.8840084, Document Type: Conference Paper, Publisher: Institute of Electrical and Electronics Engineers Inc., 2019, pp 92-95
- [2] V. Statev. The Systems Approach: a Small Tactical Unit. Security Horizons, Volume III, No. 6. Skopje, ISSN 2671-3624, DOI: 10.20544/ICP.3.6.22.p15, 2022, pp. 151-157.

- [3] I. S. Terehov, *Fundamentals of Complex Evaluation of Samples and Weapon Systems of Land Forces*, M., 1985.
- [4] V. Molhov. et al., *Mathematical Modelling of Combat Actions of the Troops*, VI, S., 1985.
- [5] S. Stanev, *Combat Capabilities and Tasks of Sabotage-Intelligence Groups of Foreign Land Forces*, *Military History Proceedings*, No. 1, 1993.
- [6] W. Swartout & J. Moore, *Explanation in Second Generation Expert Systems*. 1993, pp 543-585. 10.1007 / 978-3-642-77927-5\_24.
- [7] J. M. David, J. P. Curves, R. Simmons, *Second Generation Expert Systems – 1st Edition*, 1993, ISBN-13: 978-3540561927.
- [8] J. Sticklen., E. Wallingford *On The Relationship Between Knowledge-Based Systems Theory and Application Programs: Leveraging Task Specific Approaches*. In: David JM., Curves JP., Simmons R. (eds) *Second Generation Expert Systems*. Springer, Berlin, Heidelberg, 1993.
- [9] I. Reznik., *Fighting Capacity and Combat Readiness of the Troops: Criteria and Dialectics*, *Military Thought*, No.5, 1989, p. 53



# The nuclear family in modern terrorism

Dimo Ivanov

Land force Chair, Command and Staff Faculty  
Rakovski National Defence College  
Sofia, Bulgaria  
d.ivanov@rncd.bg

**Abstract.** *The article aims to present the relationship between the nuclear family and its involvement in modern forms of terrorism. It reveals the reasons for the emergence of family terrorism based on the inculcated belief that certain moral qualities play a major role in the upbringing within the nuclear family. It also presents the challenges which affect parenting at the nuclear family level that must find their solution before many families become victims to a particular type of terrorism, be it political, religious, ethnic, or racial. In the dynamics of the studied problem, the achievements of scientific theory and the derivation of good practices face growing demands, the need to balance the used resources, satisfy the norms of international and national law, and at the same time the growing competitiveness of terrorist organizations and networks. This gives reason and gives rise to the need for continuous scientific research despite the indisputable achievements in the field, as well as the respectable publications of several leading authors. In the interest of the research, the methods of analysis and synthesis, and temporal monitoring of open sources, including scientific publications and information media, with a wide territorial scope, were used. To further enrich the analysis, in-depth interviews were conducted with experts in the field of countering radicalization and terrorism from Bulgaria, Israel, and Great Britain. Individual cases were also analyzed using the "case study" method, or the so-called "case studies".*

**Key words:** *conscious choice, family terrorism, modern terrorism, martyrdom, nuclear family.*

## I. INTRODUCTION

The changing security environment is increasingly bringing to the fore the risks of radicalization of large societal groups and related acts of violence motivated by extremism and terrorism. The objectives of terrorist acts are to instill fear among people through civilian casualties, to attract media attention in order to propagate the ideology of extremism and terrorism [1]. In the process of examining the complex causes and aspects of the phenomenon of terrorism worldwide, several major groups of theories have been identified, namely psychological, socio-economic, politico-social and military. Such a

complex phenomenon as terrorism has many types and criteria according to which its inherent objectives, motivation, organizational structure, forces and means used, consequences, and other specific features can be defined.

## II. TYPES OF TERRORISM

Scientific classifications are needed for establishing a system of counter-terrorism measures. Some of the typical criteria used to distinguish between the different types of terrorism are based on:

- ideological - political foundations;
- territory, on which terrorist organizations operate;
- the nature of the means employed by terrorist organizations;
- the environment, in which terrorist acts take place;
- the specifics and the 'rank' of the perpetrator;
- other specific features.

When analyzing these different types and preconditions of terrorism, it is necessary to take into account that they refer to or characterize a territory or the setting in which they originate and are implemented, such as Tunnel Terrorism (Israel), Narco Terrorism (Bolivia) or Family Terrorism (Indonesia).

Terrorism is a phenomenon that possesses several specific features that give reason to define it as a global threat to the security of humanity:

- There are opportunities for terrorist acts to be carried out anywhere;
- The methods and forms of influence on the society are presupposed by the democratic values of the same society;
- The threat, generated by terrorism, requires considerable public resources to take measures for its prevention;
- Its extreme manifestations and consequences have such a negative impact on people so as to result in social

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8220>

© 2024 Dimo Ivanov. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

tension and fear that make it an effective form of violence [2].

Looking at the architecture of the normative basis for counterterrorism, three main guiding domains emerge: physical, cyber, and ideological, and a review of the different types of theories of its emergence allows one to note that each has solid evidence. In defining terrorism as a complex phenomenon, it must be acknowledged that the reason for this also lies in the factors for its emergence.

Within armed conflicts, terrorist methods are widely used usually by the side which is militarily weaker. The reason is that it is a cheap and effective way of defeating the enemy. However, the term 'enemy' includes not only a state's army and police, but also the entire civilian population.

A proof of the existence of military reasons for the emergence of terrorism is the fact that the longest existing and most active terrorist organizations are from the regions of wars and military conflicts - from the Middle East and North Caucasus. A key component and motivational tool of terrorism is the process of radicalization. The basis of any radicalization process, at personal and group level, is the sense of injustice [3].

Despite the lack of consensus on understanding the phenomenon of radicalization, this phenomenon is emerging as a consequence and result of the increasingly complex social processes in modern and postmodern societies. Similarly to any phenomenon with transnational character, it has its universal features, but also its unique and local distinctive traits [4].

### III. FAMILY TERRORISM

The proliferation of radical ideologies and the trend towards increased use of unlawful force increase the security risks in any country. Family is the smallest social unit, which is impacted in situations of uncertainty and injustice. These situations result in certain social behavior. In modern conditions, under the influence of different motives and related rules and norms, each nuclear family develops behavior consistent with their sense of belonging. Considering the nuclear family as a social unit of two parents and their children [14], we can state that they live together and develop as a unit on the basis of a common understanding of the purpose of coexistence and certain moral values. We will disclose some basic moral values that are inherent in a family.

### IV. BASIC MORAL VALUES

**Patriotism**, being one of the main moral pillars of a society, is becoming a leading moral value. For this reason, some researchers consider patriotism to be equal to the moral and to justify it as a form of consciousness. At the same time, there is a legitimate concern about the rising ideology and politics that preach superiority of one nation over another and stir up national enmity and hatred. It should be underlined that in the contemporary society there is frightening failure to distinguish between patriotism and chauvinism. Chauvinism is defined as extreme aggressive nationalism based on racism [6].

**Soldierly duty**, considered as another moral value, is not less important than patriotism. From the most ancient times, one of the most important social functions of a man

has been the protection of the family, the clan, and later - the state, from aggression. This fact makes all the more difficult to understand the persistent effort to liquidate this important quality in some form. What is the essence of this value? It is the willingness and ability to subordinate personal interests and needs to the security - personal, regional, national, or global.

Another moral significant value is **industriousness**, because it is essential for establishing a functioning organization, for discipline, clear purpose, and fairness, all of which build the team cohesion, and the nuclear family is exactly such a team. Only in conditions of elevated social significance of the organizational unit, it becomes possible the existence of this moral quality. Industriousness, takes us to the moral value of collectivism.

**Collectivism** reveals the type of human's relationship with society. It means strengthening of the community and defending its interests, and aims to develop the ability to act collectively for achieving a particular goal. This value is associated with strength, resistance, action and comprehensiveness.

**Humanism** as a moral value sounds absurd in the context of an armed conflict, because in war the participants are prepared to kill, to destroy, and to inflict physical pain, to inflict certain material damage. What kind of humanitarianism can we be talking about? Yet, humanism is measured by the ability to cooperate with other people; it is associated with compassion, recognition of the rights of others, and respect for their freedoms and dignity. It also manifests itself through intolerance to acts of violence, to rudeness or to degradation of human dignity.

### V. NUCLEAR FAMILY AND THE BASIC MORAL VALUES

All the moral values discussed above become part of the process of upbringing in the nuclear family. This process aims at the formation of personal qualities and values, attitudes towards the world, norms and forms of behavior. In addition, this process in the development of adolescents in a family is inseparable from constant change and development of attitudes in adolescents. This process undergoes three stages that take place simultaneously. The initial stage is raising awareness. Knowledge in different fields is acquired and an attitude towards knowledge is formed. The next stage is assessment-orientation stage. Knowledge from the initial stage is assessed and attitudes towards what has been learnt are formed alongside with views and beliefs. Routine behavior is formed in the third stage when the individual performs conscious actions automatically [6]. During the three stages of the process of upbringing and education, parents deprive children of their right to choose actions and push them into a world of manipulation and lies. The nuclear family is a manipulated environment in which there is only one "right" opinion and one way of "right" thinking. Thus, the opportunity for personal development and critical thinking is lost. Children need to develop in a family environment where they grow and socialize with peers. However, in terrorist organizations, the average age at which children are incited, or taken away from their families for terrorist activities, or turned

into fighters by their own parents, is 8-9 years. The young age, at which children begin to be manipulated and brought up to hatred and cruelty by their parents, is legally and morally unacceptable. The stereotypical thinking of terrorists that the status of martyr, achieved as a result of suicide bombings and the murder of innocent people, has the highest moral value, is the most serious problem that must be addressed before many more children become victims of terrorism.

## VI. DEFINITION OF FAMILY TERRORISM

The complexity of modern terrorism also depends on the considerable diversity of views on moral values. Therefore, moral values need to be described in order to analyse their purposeful formation, lest we fall under the hidden force of family terrorism. In the context of the described specifics of contemporary terrorism as well as the nuclear family, a basic definition of family terrorism can be derived. **Family terrorism is a phenomenon within the smallest family unit with a traditional or conventional structure (depending on cultural and social traditions), usually consisting of parents and their children, who become radicalized by a shared cause and use a combination of different tactical, psychological, physical, and technical methods of influence to carry out terrorist activities.**

## VII. CONCLUSION

We live in a period of rethinking fundamental views when it becomes necessary to reconsider the moral concepts and the ways in which they are formed in the family and in the society. Do we really know what is moral and what is immoral in modern life? For some this answer is negative, for others every psychological quality is moral. We are trying to answer the question whether in today's hectic life in the society, moral qualities occupy a significant leading place in the education of man, but talking about moral qualities, we cannot help asking ourselves the questions "What is morality?", "What is a moral quality and what is an immoral quality?". Without answering this question, our analysis of moral values and their formation would be incomplete and imprecise. We know that it is moral for certain individuals to serve in their country's army and defend it at all costs, and to do their life's duty honorably. For others - pacifists, saboteurs - it is moral not to touch a weapon. For others, it is moral to "play" the state.

It is difficult to give a clear and definite answer to the questions posed. In the current conditions of instability worldwide, and in the internal political life of any country, only the activity of strengthening the stability of normal coexistence, regardless of gender, religion, race or other differences, and the positive attitude towards this activity can be moral.

In recent years, we have witnessed disturbing symptoms in the expressions of patriotism of people from different societies. There has been an increase in the attitude towards neutrality and reluctance to form moral qualities. Qualities that represent the unity of a stable moral motive and an established form of behavior to satisfy it. In the role of moral motives are manifested the

consciousness of duty to the nation, the consciousness of one's own responsibility to the people, the homeland, national security, the understanding of honor, duty, good, evil, justice, personal and national dignity. On the other hand, the history of warfare, especially World War II, shows that battles to capture a city or organize its defense were common in the past [8]. Today, cities are more populated than ever, and the population is increasingly subjected to shelling and unpredictable defeats by the belligerents all conditions reinforce the process of radicalization at the individual and family level.

The report highlights the importance and role of the family environment in an individual's growth. Apart from contributing to the final shaping of an individual's biological predispositions, it also determines the behavioral patterns in their daily lives. A person's upbringing, morals and way of life, including his preferences and tastes, even his attitude towards those close to him, depend to a considerable extent on his family.

While focusing on the development of moral values in the nuclear family, whose role is important in the fight against family terrorism, we must also stress the responsibility of families towards the community with which they identify. For this reason, the social unit of the nuclear family is a key factor of the contemporary security environment in the fight against terrorism.

It is no coincidence that in all counter-terrorism forums, including the G7 meeting in Taormina, the unified position was underlined with regard to the fight against terrorism and violent extremism that the fight against terrorist acts and violent extremism, which affect all regions of the world, regardless of country, nationality or religion, remains a top priority for all governmental and non-governmental institutions in the world. [9]

## VIII. 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. Milushev, "Specifics in the construction of a security system in sites with mass residence of people", Scientific journal "Security and Defense", Year I, Issue 2, Vasil Levski National Military University, Veliko Tarnovo, Bulgaria, 2022, pp. 166-184.
- [2] L. Milushev, "Security and protection of objects with mass residence of people", Part one, ISBN 9786190112587, Textbook, "Istok-Zapad" Publishing House, Sofia, 2023
- [3] P. Marinov, "Research of the factors influencing the processes of radicalization in Bulgaria", Scientific journal "Security and Defense", Year I, Issue 1, Vasil Levski National Military University, Veliko Tarnovo, Bulgaria, 2022, pp. 148-169.
- [4] Handbook - to contract URI №5785 opm-26 5785mpd-6/ 24.01.2018 - "Conducting a national expert study on the topic: Early recognition of signs of radicalization with a

- view to implementing early prevention", under the project "Expansion of the expert capacity of the employees of the Ministry of Internal Affairs for the prevention of aggressive acts in society, corruption and radicalization", contract No. BG05SFOP001-2.004-0003-C01/27.12.2016, for the provision of grant-in-aid under the Operational Program "Good Governance".
- [5] Dictionary of Key Terms in Bulgarian Science. Vol. VI. Arts, 2019 – 2022 (extended by one year – Protocol No 3 from a meeting of the Science Council from 19.02.2021), corr. member prof. Maria Popova (freelance associate), assoc. prof. Borislav Popov (freelance associate, South-West University "Neofit Rilski"), assist. prof. Ekaterina Petkova PhD, assist. prof. Kristiana Simeonova PhD, assist. Radostina Stoyanova PhD, Adriana Hristova, [Online] Available: <https://ibl.bas.bg/en/retchnik-na-osnovnite-termini-v-balgarskata-nauka-t-vi-izkustvo/>. [Accessed: Feb. 05, 2024].
- [6] V. Drumev, "Society and its Educational Significance", "Spiritual Reading", No. VI, VII, 1881, [Online] Available: <https://posledniqt.wordpress.com/2015/03/16/васил-друмев-по-въпроса-за-обществото/>. [Accessed: Feb. 08, 2024].
- [7] D. Ivanov, "Trends in Radicalization Processes and Terrorist Activities After Covid-19", International conference "KNOWLEDGE – BASED ORGANIZATION", Vol.28, No.1, 2022, pp.66-71, Romania, <https://doi.org/10.2478/kbo-2022-0010>.
- [8] R. Marinov, S. Stoykov, P. Marinov, "Urbanized Territories Non-Existing Part of Crisis Response Operations" presented at 2019 International Conference on Creative Business for Smart and Sustainable Growth (CREBUS), Sandanski, Bulgaria, 2019.
- [9] G7 summit in Taormina, Italy, [Online] Available: <https://www.consilium.europa.eu/media/23559/g7-taormina-leaders-communique.pdf>. [Accessed: Feb. 20, 2024].
- [10] D. Ivanov, "Using non-verbal communication in counter-terrorism operations", ISSN 2367-7473, Proceedings, Scientific Conference "Current Security Issues", Vasil Levski National University, Veliko Tarnovo, Bulgaria, 2022.
- [11] K. Gradev, P. Marinov, D. Ivanov, Analysis of the Operational Environment for the Land Force Units Participation in Stabilisation Operations, *Voenen Zhurnal* (ISSN 0861-7392) scientific journal is being printed four times per year: Issue 1 (January – March); Issue 2 (April – June); Issue 3 (July – September); Issue 4 (October – December), issue 3-4/2022, volume 129, pp. 234-254.
- [12] P. Marinov, S. Stoykov, D. Ivanov, "Theoretical foundations of terrorism and anti-terrorism", Part one, ISBN 978-619-01-1243-3, Textbook, "Istok-Zapad" Publishing House, Sofia, 2023, pp. 175-206, pp. 284-303
- [13] D. Ivanov, "Family Terrorism or a Conscious choice", ISSN: 2815-388X - Print, ISSN:2815-4584 - Online, page 23-37, Scientific journal "Security and Defense", Year II, Issue 2, Vasil Levski National Military University, Veliko Tarnovo, Bulgaria, 2023
- [14] Cambridge Dictionary - Make your words meaningful, [Online]. Available: <https://dictionary.cambridge.org/dictionary/english/nuclear-family>, [Accessed: Feb. 21, 2024].

# Methodology For Testing Physical Samples (Models) Of A Chemical Power Source Intended For Single Use In Defence Industry Products

**Galina Hristova Ivanova**

“Vasil Levski” NMU  
“Security and Defense” Faculty  
Veliko Tarnovo, Bulgaria

galina\_h\_ivanova@abv.bg, V.Tarnovo, bul. Bulgaria, 76

**Ivan Nikolaev Minevski**

“Vasil Levski” NMU  
“Logistic and tehnologie” Faculty  
Veliko Tarnovo, Bulgaria

ivan\_minevski@abv.bg, V.Tarnovo, bul. Bulgaria, 76

**Abstract.** *The proposed and developed methodology is designed to determine the indicators of reliability and operability of disposable chemical power sources. It is recommended for conducting tests of physical samples (real models) under various environmental impacts, under mechanical-dynamic loads, as well as in various operating conditions. The methodology includes subjecting the samples to testing the impact of destabilizing factors of the environment in order to determine their workability and reliability. Conducting this independent test is required due to the importance of the power source and in order to obtain sufficient statistical information about the reliability of its electrochemical elements. To ensure the completeness and comprehensiveness of the study, an additional methodology has been compiled – Methodology for Identification of Physical Models of a Power Source.*

**Key words:** *methodology, physical samples, destabilizing factors.*

## I. INTRODUCTION

The purpose of the Methodology is to subject to testing chemical power sources applicable in defence industry.

This methodology is implemented in accordance with the following specifications and safety aspects:

- the electro-chemical elements used for building the power sources (PS) and the power sources themselves should be designed so that they can operate without creating conditions for temperature higher than the critical temperature specified by the manufacturer;
- the electro-chemical elements used as well as the power sources should be designed so that a brief short circuit is avoided in normal conditions of exploitation and during transportation;
- each individual power source should be designed so that the same electro-chemical elements are used from the same manufacturer, and the usage of constructive

elements from different manufacturers in one and the same sample is forbidden;

- lithium power sources containing lithium elements or sequence of elements connected in parallel should be equipped efficiently so that they can prevent reverse current, jacket swelling or casing rupture.

## II. MATERIALS AND METHODS IN TESTING PHYSICAL SAMPLES OF POWER SOURCES

The tests of the electro-chemical systems containing the chemical element lithium (Li) are conducted subject to additional conditions. They are specified depending on the amount of lithium (Li) in the tested elements. The testing of these physical models (experimental samples) is considered as an individual type, and they are subject to additional tests depending on the mass of lithium in them. When the lithium (Li) is more than 0.1 g or when it is more than 20 % of the total mass, regardless of where it is contained – in the electrodes or the electrolyte, additional tests of the samples are conducted. The sets of electrochemical elements in the power source (battery) containing more than 500 g of lithium are not subject to testing provided that they have been assembled using electrical bonding. The power sources must have gone through all necessary tests or be equipped with a system capable of controlling the pressure in the assembly and preventing short circuits.

The selection of samples for testing includes each individual type of electrochemical elements and power sources which are to be tested by means of developed physical models. To conduct the tests, physical samples (models) of power sources have been developed. They were used to perform tests of reliability indicators of the electrochemical systems that make up the power source. The number of physical samples of power sources needed to perform the tests are indicated in Table 1 [1].

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8203>

© 2024 Galina Hristova Ivanova, Ivan Nikolaev Minevski. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

TABLE 1 NUMBER OF SAMPLES SUBJECT TO TESTING [1]

Primary elements and batteries				
Number of samples T-1 – T-5	Elements		Batteries	
	10 elements	10 elements	5 batteries	5 batteries
Number of samples T-6	Elements		Batteries	
	5 elements	5 elements	5 compound	5 compound
Number of samples T-6	Elements		Batteries	
		10 elements	Tests are not mandatory.	

The tests are repeated if they prove that the primary lithium elements or the power sources assembled with them do not correspond to the requirements set by the tactical-technical assignment (TTA). Before the tests are repeated, the necessary measures must be taken to eliminate the fault or faults leading to failure in the conducted tests.

### III. RESULTS AND DISCUSSION

*Safety instructions* – in conducting the indicated tests, procedures are used which may result in injuries if the necessary safety measures are not taken.

*Temperature of the environment* – if nothing else has been indicated, all tests are to be conducted in room temperature of  $20 \pm 5$  °C.

*Permissible error when measuring parameters* – the total error of the controlled and measured values should be within the following interval:

- a/  $\pm 1$  % – for the voltage;
- b/  $\pm 1$  % – for the current;
- c/  $\pm 2$  °C – for the temperature;
- d/  $\pm 0,1$  % – for the time;
- e/  $\pm 0,1$  % – for the dimensions;
- f/  $\pm 1$  % – for the capacity.

The given limit values also include the combined values of the error of the measuring instruments, the error of the used technology of the conducted measurement and other sources of error arising in the process of conducting the tests.

The electrochemical elements used are subjected to an external inspection and should meet the optimal characteristics and safety determined by the manufacturer [2].

#### A. Evaluation of the test results of power sources

- *Displacement* in the test process occurs if one or more electrochemical elements of the power source, during the test, have fallen out of their package, changed their position inside the package or there is a displacement of the elements relative to each other.

- *Deformation* of the electrochemical elements and power sources (batteries), in the process of their testing, happens if there is a change in their physical dimensions by more than 10%.

- A *short circuit* in the test process occurs if the values of the voltage of the open circuit of electrochemical elements or the power source, after the

test is completed, is less than 90 % of the value measured immediately before the test. This requirement does not apply when the complete discharge of the electrochemical elements or the power source (battery) built with them is subjected to the test.

- *Overheating* of electrochemical elements and power sources in the test process occurs if the housing external temperature exceeds the temperature of 170°C.

- The *mass loss* of electrochemical elements and power sources  $\Delta m/m\%$  is calculated by formula 1:

$$\Delta m/m = \frac{m_1 - m_2}{m_1} 100 \%, \quad (1)$$

$m_1$  – mass before the test, g;

$m_2$  – mass at the end of the test, g.

- *Airtightness violation* is considered if, during the test, there has been gas leakage from the tested electrochemical elements through a device designed to reduce the internal pressure. The exhaust gas may contain entrained particles.

- *Ignition* of the electrochemical elements and power sources, in the process of testing, occurs if a fire is observed coming out of them.

- *Destruction* of electrochemical elements or power sources, in the test process, occurs when mechanical destruction of the housing is observed, which is accompanied by the release of gas or the leakage of electrolyte, but there is no release of internal solid materials from their composition.

- An *explosion* in the test process takes place if penetration of solid particles is observed from the electrochemical element or the power source through a mesh screen made of tempered aluminium wire with a diameter of 0.25 mm with a mesh density of 6 - 7 wires per 1 cm, placed at a distance of 25 cm from them [3].

#### B Transportation testing of physical samples of power sources designed as a defence product

The presented Table 2 provides an overview of the conducted tests and the set requirements for power sources and their constituent elements. To ensure safety during transportation and in cases of improper use of the electrochemical elements and power sources, it is necessary to conduct a test of their packaging. According to the proposed methodology, transport tests include:

TABLE 2 TESTS AND REQUIREMENTS TO TESTING SAMPLES [3]

Indication of	Name	Requirements
Transportation requirements	T-1	Altitude HM(NM); HЭ(NL); HГ(NV); HK3(NC); HP(NR); HB(NE); HO(NF);
	T-2	Temperature cycle HM(NM); HЭ(NL); HГ(NV); HK3(NC); HP(NR); HB(NE); HO(NF);
	T-3	Vibrations HM(NM); HЭ(NL); HГ(NV); HK3(NC); HP(NR); HB(NE); HO(NF);
	T-4	Shock HM(NM); HЭ(NL); HГ(NV); HK3(NC);

			HP(NR); HB(NE); HO(NF);
T-5	External short circuit		HT (NT); HP(NR); HB(NE); HO(NF);
T-6	Dynamic load		HT (NT); HB(NE); HO(NF);
<b>Abbreviation code:</b> HM(NM) – absence of mass loss; HK3(NC) – absence of external short circuit; HИ(ND) – absence of deformations; HB(NE) – absence of explosion; HO(NF) – absence of burning; HО(NL) – absence of leaks; HP(NR) – absence of destruction; HИ(NS) – absence of displacement; HT(NT) – absence of overheating; HГ(NV) – absence of airtightness violation;			

### 1. Testing T-1: Altitude

a) *Purpose:* Testing T-1: Altitude models transport by air in low ambient pressure conditions.

b) *Conducting the test:* The power sources are placed in a chamber with a temperature of  $0 \pm 2$  °C reached. The pressure is reduced to a value of  $19.20 \pm 0.31$  kPa (145 Torr). The duration of the stay is 40 min. The voltage values of the tested products are measured, and the duration of the test is 10 min. Then, the temperature and air pressure in the chamber with the experimental samples are increased to values under normal climatic conditions:  $T = 20 \pm 5$  °C and atmospheric pressure  $101.32 \pm 0.31$  kPa (760 Torr) again with a duration of 10 min. The temperature of the tested products is stabilized at  $20 \pm 5$  °C for 30 min. The indicators of the tested products are measured.

c) *Requirements:* In the process of testing electrochemical elements and power sources, there should be no loss of mass, electrolyte leakage, airtightness violation, brief short circuit, destruction, explosion or burning.

### 2. Testing T-2: Temperature cycle

a) *Purpose:* The test is designed to evaluate the integrity of assemblies, airtightness, and internal connections of electrochemical elements and power sources. The test is carried out in a temperature cycle.

b) *Conducting the test:* The experiment is conducted after the temperature of the tested power sources has stabilized at a temperature of  $17.8 \pm 0.1$  °C for 2 (two) hours. The voltage of the tested power sources is measured at idle.

Conditions for conducting a test for one cycle:

The indicators of the power sources are measured after placing them in a chamber and reaching a temperature of minus  $40 \pm 2$  °C for 30 min. The voltage of the tested products is measured at idle speed for 2 min. The power sources are placed in a chamber at a temperature of  $50 \pm 2$  °C. The duration of exposure to the specified temperature is 30 min. The technological time of moving the tested products from one chamber to the other is  $2.3 \pm 0.1$  min. The measurement of the studied indicator (electrical voltage) of the tested products at idle speed is about 2 min. The total time for testing one of the products in one cycle is 1 h and 6 min [4, 5].

c) *Requirements:* In the process of testing electrochemical elements and power sources, there should be no loss of mass, electrolyte leakage, airtightness

violation, brief short circuit, destruction, explosion or burning.

### 3. Testing T-3: Vibrations

a) *Purpose:* The specified test models the impact of vibrations during transportation of electrochemical elements and power sources. The test conditions are based on the range of vibrations (vibration stress) during service handling and transportation of the elements and power sources.

b) *Conducting the test:* The electrochemical elements and power sources under test must be firmly fixed to the platform of the vibration test device without being deformed, but also so that the vibrations are transmitted as accurately as possible. The test items are subjected to sinusoidal vibration in accordance with Table 3. This cycle is repeated up to 6 times in each of the three mutually-perpendicular directions. One of the directions must necessarily be perpendicular to the surface of the test sample with electrical terminals [6].

TABLE 3 PARAMETERS OF SINUSOIDAL VIBRATIONS [6]

Range of frequency		Amplitude	Duration of the logarithm	Axes	Number of cycles
From	to				
$f_1 = 7\text{Hz}$	$f_2$	$a_1 = 1\text{gn}$	15 min	X	12
$f_2$	$f_3$	$s = 0.8\text{mm}$ m		Y	12
$f_3$	$f_4 = 200\text{Hz}$	$a_2 = 8\text{gn}$		Z	12
and return frequency $f_1 = 7\text{Hz}$				Total time	36
<b>Note:</b> Vibration amplitude – this is the maximum absolute value of displacement or acceleration. For example, a displacement amplitude of 0.8mm corresponds to a displacement scale of 1.6mm. Abbreviation code: $f_1$ and $f_4$ – lower and upper frequency; $f_2$ and $f_3$ – transition frequencies; $a_1$ and $a_2$ – acceleration amplitude; $s$ – displacement amplitude.					

c) *Requirements:* In the process of testing the elements and batteries, there should be no loss of mass, electrolyte leakage, airtightness violation, brief short circuit, destruction, explosion or burning.

### 4. Testing T-4: Shock impact

a) *Purpose:* This test simulates a sharp mechanical impact on the elements or batteries during transportation.

b) *Test conducting procedure:* The test items shall be securely fastened to the test rig by means of fasteners securing all mounting surfaces of each test item and battery. They must be subjected to three shocks in each of the three mutually-perpendicular mounting positions. The parameters of each stroke must correspond to the data in table 3.

TABLE 4 PARAMETERS OF THE SHOCK INTENDED FOR TESTING [7]

Product type	Wave type	Maximum acceleration	Impulse length, ms	Number of shocks
Small	semi-sinusoidal	150 gn	6	3
Big	semi-sinusoidal	50 gn	11	3

c) *Requirements:* In the process of testing the elements and batteries, there should be no loss of mass, electrolyte leakage, airtightness violation, brief short circuit, destruction, explosion or burning.

#### 5. Testing T-5: External short circuit

a) *Purpose:* The test simulates the state of an external short circuit.

b) *Conducting the test:* Tested cells and batteries are stabilized at external temperature and then subjected to a momentary external short circuit. The samples are monitored for 6 hours after the end of the exposure [8].

c) *Requirements:* In the process of testing and monitoring the samples during all the 6 hours, there should be no overheating, destruction, explosion or burning.

#### 6. Dynamic load (impulse shock)

a) *Purpose:* The test simulates an external short circuit.

b) *Conducting the test:* Test cells and batteries are placed on a flat metal plate. Each component of the battery must be subjected to one dynamic shock. The test samples were observed for 6 hours after the final impact. Products that have not passed other transport tests are subjected to this test [8].

c) *Requirements:* In the process of testing and monitoring the samples during all the 6 hours, there should be no overheating, destruction, explosion or burning.

#### C Safety measure when conducting the tests

When conducting the tests, the necessary safety measures must be observed. The normal operation of power sources is associated with the release of a certain amount of heat into the environment. Depending on the operating mode of the product and the possibility of heat transfer to surrounding objects, overheating, burning or explosion may occur. For this reason, it is recommended to use safety glasses, clothes and gloves, and if there is a risk of exploding the test object, the experiment should be carried out behind safety glass.

The defective condition of the electrical equipment in the test laboratory or its improper handling can lead to accidents or be the cause of fire or explosion.

Current up to 36 V has been found to be safe, and therefore, all portable electrical equipment in the laboratory must operate at 12 V (the tested power sources have a nominal voltage of 12 V).

The methodology is designed to prove the performance of batteries built from different electrochemical systems. The proposed tests are aimed at batteries intended for single use.

#### D Methodology for identification of physical models of the power source

According to the limitations set in the methodology, the tested physical samples (batteries) of a product for the defence industry are intended for single use. The components from which the experimental samples are built are identical, except for the chemical composition of the power source. The electrochemical elements that make

up the power sources of the physical models are made up of three electrochemical systems – manganese-zinc, silver-zinc and lithium. The choice of the type of electrochemical cells used is dictated by their availability and variety of sizes.

The main task of the proposed methodology is related to the possibility of correct identification of each physical model during laboratory tests. Therefore, each of them should be labelled starting from the type of electrochemical system used. The characteristics of the elements that make up the electrochemical system are also described – electrodes, electrolyte, separators, and, if possible, the chemical reactions taking place.

a) Electrochemical systems used for building the power source of the physical models of the product

The following electrochemical systems designed for a disposable power source have been developed and prepared for testing:

- Chemical current sources intended for single use based on manganese and zinc, which can be with salt or alkaline electrolyte. In manganese-zinc current sources with salt electrolyte  $\text{Zn}|\text{NH}_4\text{Cl}|\text{MnO}_2$ , the battery case is also an **anode** (made of Zn), the active substance of the **cathode** is electrolytic manganese dioxide ( $\text{MnO}_2$ ) or chemical manganese dioxide,  $\text{NH}_4\text{Cl}$ ,  $\text{ZnCl}_2$  or a mixture of the two substances is used as an **electrolyte**. The electrolyte is located in the thickened areas or in a microporous separator. To reduce the corrosion rate of zinc, corrosion inhibitors are added to the electrolyte. The advantages of these sources of electric current (batteries) are related to the low price and the large number of sizes, the relatively simple production technology and the readiness to be used immediately. The disadvantages are related to the downward discharge curve during operation, the relatively low specific energy released, and a significant drop in performance at high load and low temperatures.

Manganese-zinc power sources are also produced with alkaline electrolyte  $\text{Zn}|\text{KOH}|\text{MnO}_2$ . They use powdered Zn as **anode** and  $\text{MnO}_2$  as **cathode**. The **electrolyte** is a gel solution of KOH or KOH in a matrix. Corrosion inhibitors are included in the composition of the anode and electrolyte. Compared to salt electrolyte power sources, alkaline ones have a higher capacity and energy density in operation, especially at high loads and low temperature, but have a higher price value [9].

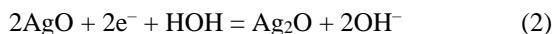
- In the silver-zinc primary cells  $\text{Zn}/\text{Ag}_2\text{O}$  or  $\text{Zn}|\text{KOH}|\text{Ag}_2\text{O}, \text{Ag}^+$ , powdered zinc is used for the **anode**, silver oxide for the **cathode**, and KOH or NaOH solution for the **electrolyte**. Silver is reduced on the cathode from Ag(I) to Ag(II) during operation of the chemical current source (the battery), i.e. in the discharge mode, the alkaline electrolyte is used as a donor of hydroxyl groups, and the following electrochemical processes take place:

- an oxidation reaction of zinc metal takes place at the anode:



- the following reaction takes place at the cathode:





i.e. a reduction reaction of the divalent silver ion to a monovalent ion and subsequently to pure silver occurs according to the scheme:



the total equation is written in the form:



Silver power sources (batteries) of this type have a horizontal discharge curve, high energy density and low self-discharge. They can work at high loads, but the disadvantage is the high cost of their components.

- Lithium primary current sources with a **solid cathode and aprotic electrolyte**, the reducing agent is lithium, and the oxidizing agent is metal oxides, sulphides, or fluorocarbons. The **electrolytes** are solutions of lithium salts ( $\text{LiClO}_4$ ,  $\text{LiBF}_4$  or  $\text{LiBr}$ ) in aprotic solvents. In lithium current sources with **liquid or dissolved oxidant**  $\text{Li}|\text{LiBr}|\text{SO}_2$  and  $\text{Li}|\text{LiAlCl}_4, \text{SOCl}_2|\text{SOCl}_2$ , the cathodes in the electrochemical current source are insoluble and made of carbon materials deposited on aluminium (for  $\text{SO}_2$ ), based of nickel steel or stainless steel. The **electrolyte** in lithium sulphur dioxide cells is  $\text{LiBr}$  dissolved in acetonitrile; in the elements with thionyl chloride and sulphuryl chloride –  $\text{LiAlCl}_4$   $\text{SOCl}_2$  or  $\text{SO}_2\text{Cl}_2$  with additives.

Lithium primary electrochemical current sources have higher capacity and energy density, a wider operating temperature range, better performance at lower temperatures, and a lower self-discharge rate compared to the same parameters of manganese-zinc sources of power supply. Their main drawback is their high price. Lithium primary sources of electrochemical current are used in medical, industrial and military electronics.

b) Specifying the reliability and operability requirements for the power sources

When designing the power sources (batteries), the requirements for their reliability and operability are of great importance. These two indicators are affected by the magnitude of the electric current and the electric voltage, as well as the duration of the operation of the final product. It is also essential to determine correctly the storage period of the power source before it is put into use. The requirements for the constructed and tested power sources can be summarized as follows:

- electrical voltage from 6 to 15 V and more;
- nominal load current from 10  $\mu\text{A}$  to 1 A and more;
- working time from 1 ms to 60 min and more;
- operability in a temperature range from minus 40 °C to plus 50 °C;
- storage period from 5 to 20 years.

One of the most important requirements for the power sources is their high reliability when working in conditions of high accelerations that occur at the time of their operation.

c) Building and numbering the power sources of the

physical model

Depending on the physical parameters of the power source, the elements of the appropriate size are selected. This is done during their construction, depending on the offered sizes, operating characteristics and indicators of the building electrochemical elements.

The first power supplies are developed for research purposes and are made of manganese-zinc electrochemical elements (alkaline elements) and silver-zinc electrochemical cells, which are denoted LR and SR, respectively. According to the different standards, the used building electrochemical elements are marked as model: LR44; SR44; A76; SR44SW; AG13; SG13; LR154; S76; EPX76; 157; 303 or 357. They have a weight of 1.8 g, a diameter of 11.6 mm, a height of 5.4 mm, a nominal voltage of 1.5 V and a capacity of 110 – 125 mAh. Lithium power sources are also presented, and they are denoted by CR, and CR-1/3N model elements were also used for their construction. The latter have a diameter of 11.6 mm, a height of 10.8 mm, a nominal voltage of 3 V and a capacity of 170 mAh.

Eight 1.5 V electrochemical cells or four 3 V lithium electrochemical cells were used to construct the power source. The resulting final rated voltage was 12 V.

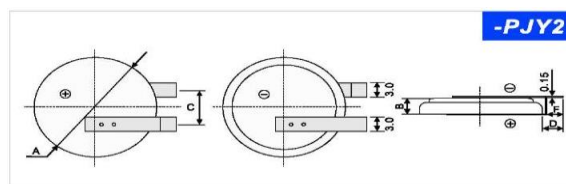


Fig. 1. Connection type used when constructing the physical power source models

The P-JY2 series connection between the electrochemical elements in the power source is made with nickel-plated connection plates of the AA-4-20-13R type with a thickness of 0.13 mm and a width of 4 mm. An ARM-10KAS spot welding machine was used.

In parallel with the construction of the physical samples, a visual model was also built. With its help, the position of the electrochemical elements, the location of the connecting elements, the size of the channel for the connecting wires and, last but not least, the dimensions of the final model (sample) were determined in 3D space.

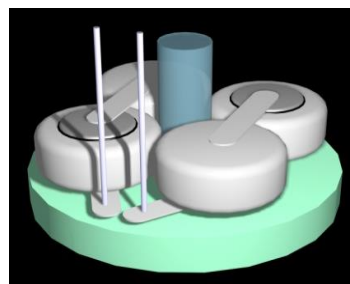


Fig. 2 Visual 3D model of a power source built with 4 electrochemical elements on one level [10]

The conducted experiments and the positive results shown by the tested physical models of the power source necessitate the transition to the stage of development of a sample made up of two levels of electrochemical elements

and, accordingly, a virtual sample of the proposed power source.

The numbering of the power sources intended for physical samples of the product is carried out according to a developed numbering system.

It is based on the type of electrochemical elements used, their size and operating voltage.

To indicate the type of the electrochemical system of the elements, the designation LR is used for manganese-zinc elements, SR – for silver-zinc elements, and CR – for lithium elements.

The following system is proposed for numbering the power sources (batteries) related to their identification during the tests:

1. The batch number is indicated in brackets, and it consecutively includes: the year and month of creation of the power source (PS); the type of electrochemical system (respectively for LR it is indicated by the number 1, for SR – by the number 2, and for CR – by the number 3), and the serial number of the power source in the batch.

2. The model of the electrochemical elements, when it is different from the one specified, is written after the batch number in brackets.

3. The manufacturer of the electrochemical elements is specified at the end of the identification number, after the brackets.

The serial number obtained from the power source is printed on the housing. It is entered during the tests and serves to compare the achieved results.

#### IV. CONCLUSIONS RELATED TO THE PROPOSED METHODOLOGY

The methodology is recommended when testing physical samples (real models) as part of a product intended for the defence industry. The tested samples are subjected to various environmental influences and mechanical-dynamic loads. The tests are selected depending on the expected conditions of transportation, storage and operation of the final product and the specified requirements in the tactical-technical task (TTT) for it.

As required, the power source samples used and developed are exact models of the final product. The methodology envisages that they should be tested for the impact of destabilizing environmental factors in order to determine their operability and reliability. Conducting this independent test is required due to the importance of the power source to guarantee the operability of the entire

product and in order to obtain sufficient statistical information on the reliability of the electrochemical elements that make it up. In connection with this, it is appropriate to test three electrochemical types of power sources (alkaline, silver and lithium). They differ in the electrochemical elements used for their construction – their electrochemical composition, sizes, and performance characteristics. The proposed Methodology for Identification of the Physical Models of a Power Source makes it easier to work with them.

With the developed Methodology, a series of physical samples were tested, and the results shown satisfy the requirements of the specifications.

#### ACKNOWLEDGEMENTS

The paper was financed by the National Scientific Program 'Security and Defence' of the Ministry of Education and Science of the Republic of Bulgaria, in implementation of the Decision of the Council of Ministers of the Republic of Bulgaria № 731/21.10.2021 and under Agreement № D01-74/19.05.2022. Work task 3.1.1. Research and application, in the field of security and defence, of renewable and chemical sources of electricity and the possibilities of using non-volatile sources based on lithium.

#### REFERENCES

- [1] Bulgarian State Standard BDS 2.601. Unified system for construction documentation. Operational documents.
- [2] Bulgarian State Standard BDS EN ISO 9000:2001. Quality management systems Sofia February 2007.
- [3] State Standard GOST R IEC – 62281-2007. Safety when transporting primary lithium elements and batteries, lithium accumulators and accumulator batteries.
- [4] Bulgarian State Standard BDS EN 60068 – 2-21:1999. Environmental testing. Part 2-21: Tests. Test U: Robustness of terminations and integral mounting devices.
- [5] Bulgarian State Standard BDS EN 60068 – 2-33:2003. Environmental testing. Part 2-33: Tests. Guidance on change of temperature tests.
- [6] Bulgarian State Standard BDS EN 60068 – 2-6:2007. Environmental testing. Part 2-6: Tests. Test Fc: Vibrations (sinusoidal).
- [7] Bulgarian State Standard BDS EN 60068 – 2-27:2003. Environmental testing. Part 2-27: Tests. Test Ea and guidance: Shock.
- [8] Bulgarian State Standard BDS EN 60068 – 2-14:2009. Environmental testing. Part 2-14: Tests. Test N: Change of temperature.
- [9] Churikov, A., Kazarinov, I. Modern chemical sources of current. Saratov, 2008.
- [10] Autodesk 3DS MAX 2015 software – Default Scanline Renderer.

# Development Of A Program For Conducting Tests With Physical Samples Of A Defence Industry Product

**Galina Hristova Ivanova**

National Military University "Vasil Levski"

"Security and Defense" Faculty

Veliko Tarnovo, Bulgaria

galina\_h\_ivanova@abv.bg, V.Tarnovo, bul. Balgaria, 76

**Abstract.** The developed Program for Conducting a Test with Physical Samples of a Defence Industry Product is a systematic approach to scientific research related to the study, research, and collection of various types of data (information) on the researched object. The constructed and subjected to testing physical samples (models) of the product are used to confirm the correctness of the initial assumptions made. They are related to the possibility of improving the final product without changing the basic requirements for it. The search for an appropriate solution to the research task is related to the construction and testing of a new type of details. They are related to the accumulation of reliable spatial-geometrical data about the product and its reliability characteristics. In addition, to improve the visual perception of the physical objects, a Visual 3D model of the tested physical samples of a chemical power source (batteries) was developed and presented in the report using the capabilities of modern digital programs.

**Keywords:** 3D model, physical samples, testing.

## I. INTRODUCTION

The Plan for the design, manufacture and testing of physical samples of a defence industry product fulfils its functions by tracking all the main stages related to the commissioning of a defence product. It gives consistency, analogy and systematicity to the stages of the research while providing an opportunity to collect, systematize and evaluate the information obtained.

The information is used to study the material objects and the physical processes taking place with them. The studied object (physical model) should not be perceived only as a specific physical object but as a system consisting of various interconnected objects and phenomena. Knowing their totality determines the reliability of the product and its components.

The plan was drawn up on the basis of an in-depth study on the possibility of determining the reliability

characteristics and their influence on the working mode of the products. It aims to trace and justify the main stages of the scientific research related to the development and testing of physical samples (models) to prove their reliability, operability and safety.

## II. MATERIALS AND METHODS

Scientific research and didactic methods were used in the development of the Program for testing physical samples of a defence industry product. The literature used is within the relevant volume, and literary sources and the requirements for the research object specified in them are used for summary and analysis. The Program aims to offer an option for a logical sequence of stages in conducting tests with physical samples and to justify key points in the scientific research (Fig. 1). When presenting the results, didactic methods, taxonomic categories, as well as methods of selection and comparative analysis were used.

A software method was used to visualize the developed physical samples (Fig. 2), and for additional visualization of the research object, visual models of the interior of the power source, indicated in Figures 3 to 5, were built using a computer visualization program. The above-mentioned Program is a theoretical development that guides the conduct of a practical examination of products from the defence industry and structures the main elements in the conduct of this examination, specified in section III.

## III. RESULTS AND DISCUSSION

The main goals set by the Program are related to structuring the stages in current and future developments, starting from the conceptual design to the construction of the final product. The core structure of the content concerns the main categories in the taxonomy – *knowledge, understanding, application, analysis,*

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8204>

© 2024 Galina Hristova Ivanova. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

*synthesis, evaluation.* Evaluative content is given on the basis of predefined criteria, selection of own evaluation criteria and their argumentation through examples presented in the figures in the paper.

Using B. Bloom's taxonomy, the following contributions can be formulated, which correspond in essence to its different levels. In the initial stage, a conceptual project is formed, which unites a certain category of *knowledge* through the possibility of grouping and defining the main task. To *understand* the essence of the problem, we choose a sequence of actions related to getting to know the characteristics of the studied object. Through direct research actions, an *application of the studied object* is sought, it is illustrated, constructed, demonstrated, proved, or an experiment is conducted. In order to *carry out an analysis*, we group, separate, select, reveal, grade or predict the characteristics of the researched object. The proposed program implies the use of the taxonomic category for the *synthesis* of acquired knowledge through its documentation, systematization, combination, modification, planning, modelling, design and presentation. Giving an *assessment* and its reasoning are the basis for determining the application, ergonomics and operability of the final product [1].

Fig. 1 presents a generalized algorithm of the sequence of stages that make up the Plan for the design, manufacture and testing of physical samples of a non-contact radio proximity fuse (VN-RL-82). The main tests to which the physical models are subjected are also indicated.

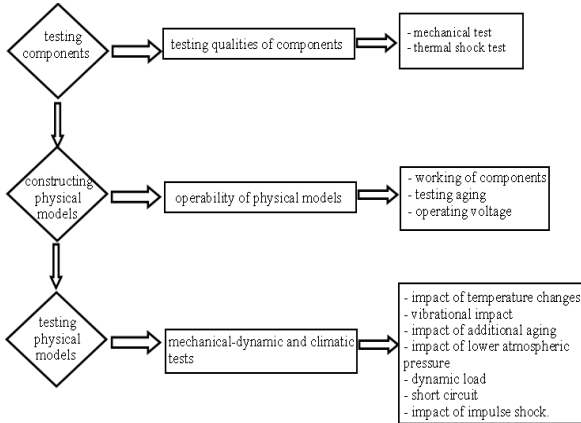


Fig. 1. Algorithm for conducting the testing of the constructed physical models

During the tests, in order to specify a certain characteristic of the final product, it is allowed to conduct additional tests to those indicated in Fig. 1.

#### A. Object and area of application of the plan

The presented plan determines the order of development, construction and testing of physical models (samples) of defence products (products and materials). It indicates the main requirements related to the implementation of verification and control and gives the value range of the conducted tests. It includes references and prescriptions from the standards listed below, their latest editions being valid.

– Bulgarian State Standard BDS 2.503 Unified system for construction documentation. Amendment Rules [2];

– Bulgarian State Standard BDS 2.601 Unified system for construction documentation. Operational documents [3];

– Military Standard VS 40069 Tactical-technical assignment [4].

#### B. Terminology and definitions used in the plan

*Defence product* – general name for a product or material whose purpose is to satisfy the needs of the ministry of Defence.

*Products* – products whose quantity is measured in pieces (specimens). The products are characterized by the fact that they have a resource that is used up during their operation.

*Materials* – products whose quantity is measured in units of length, area, volume, or mass (m, m<sup>2</sup>, m<sup>3</sup>, kg, etc.). They do not have a resource, but during their use, the materials themselves are used up.

*Representatives of the contracting authority* – a group of specialists for scientific and technical support tasked to check and agree the documentation, control the development and accept the defence products at the various stages of their development, implementation and production.

*Contracting authority* – the people under whose initiative the research is conducted.

The terminology dictionary has been created based on Military Standard VS 2.03:2007 – Development and implementation in the production of defence products – MoD № OH 736/16.11.2007 [5].

#### C. General conditions and main stages in the test program

The main concept project is related to the opportunity stated by the contracting authority for the accumulation of scientific research data for the construction, testing and improvement of a non-contact radio proximity fuse through the construction of physical samples for laboratory tests.

The plan divides the research process related to the collection and processing of information about the research object into standardized and unified stages. This is how purposeful management of the information processes related to the implementation of the task is carried out.

The main stages and activities in the construction, development and testing of the physical samples (models) and their components (mechanical part, power source and electronic part – considered as components of a defence product) are as follows:

*First stage: Concept project (for the product)* – it includes the development of the idea for an upgrade to a defence industry product, improvement of its mechanical part, and design of a modern electrochemical power source;

*Second stage: Working project (for the product) and laboratory technology (for the materials)* – this stage is related to constructing and conducting of the initial testing

of the materials which the product is made of, as well as the creation of a visual 3D model;

*Third stage: Testing sample (for the product) and testing batch (for the materials)* – it is related to conducting the initial tests for the operability and capability of the product to perform the tactical-technical task or the production of an experimental batch of materials to be subjected to testing.

*Forth stage: Testing batch (for products) and testing batch (for materials)* – the purpose is to construct an experimental batch of fully constructed physical samples (models) of the product and an experimental batch of materials to be tested in a certified laboratory for reliability, operability and safety. The compatibility of the product with the requirements of the tactical-technical task is examined, taking all precautionary measures for the safe conduct of the tests (the product subjected to testing does not contain explosive substances) [6, 7].

a) *Concept project for the product*

The purpose of the concept project is to clarify the basic principles of operation and the possible options for technical design of the product and its constituent parts. An assessment is made which of the developed options will most fully satisfy the tactical-technical task. During the implementation of the concept project, research and development activities are carried out. They are carried out through research and experiments in a volume necessary to confirm the possibility of improving a non-contact radio proximity fuse and developing a modern power source based on selected conceptual solutions.

The tasks set for implementation of the concept project have been started through the development and construction of three variants of a chemical power source for a non-contact radio proximity fuse. A representation model and physical models of a power source and its components have been developed, researched and tested in order to justify the possibility of realizing the concept project. A technological and technical-economic analysis of the proposed options is carried out. An assumption is made about the possibility of improving a defence product.

Point *E* of this paper presents the developed 3D models of the chemical power sources, which are part of the concept project and are yet to be tested.

b) *Working project for the product*

The purpose of the working project is to determine the main technical characteristics of the product and its components, based on an approved conceptual design, through the production and testing of models (samples). An opportunity is being sought to confirm the technical characteristics and to meet the requirements of the tactical-technical task in the experimental production [8].

During the development of the working project, activities necessary to obtain a complete understanding of the design of the product being developed are carried out, an assessment is made of its compliance with the tactical-technical task, and its technology and complexity are taken into account. The indicators of ergonomics (method of packaging and transportation) and operation are defined

and discussed to meet the technical requirements of safety and occupational hygiene. This is achieved by building and researching physical models that fully and accurately repeat the real characteristics of the final product.

In general, during the development of the working project, the researcher performs the following main activities:

- Develops and substantiates the technical characteristics and studies the principle of operation of the product and its components, meeting the requirements of the tactical-technical task (TTT).

- Compiles the necessary principle diagrams of the product building components and determines the dependence between the electrical or mechanical connections in them.

- Analyses the design of the product, its technology and the extent to which it complies with the operating conditions.

- Assesses to what extent the approved design characteristics provide the possibility of creating unification and improvement of the products.

- Confirms meeting the technical requirements and economic indicators defined in the TTT.

- Makes assessment of the possibility of meeting the requirements of reliability and operability tested in TTT.

- Finalizes the technical tasks and requests for the development of new assembled units, components and materials.

- Evaluates the possibility of transportation, storage and installation of the product at the place of operation.

A program and a methodology for conducting the tests of the samples are developed in accordance with the regulatory documents defined as the basis for proving the reliability of the product [9].

A batch of experimental physical models (samples) is produced for testing in a certified laboratory. They are submitted to the laboratory and are approved, designed and built (in the necessary amount) so that their compliance with the requirements laid down in the TTT of the product can be confirmed. To conduct the tests, the presented physical models must fully correspond and repeat the characteristics of the object being tested. An analysis of the test results is prepared, on its basis it is possible to refine and correct the working project in accordance with the final decisions. This stage is related to experimenting and defining the main characteristics of the product to determine its reliability. It is seen as an initial period of development, during which the intensity of failures is increased due to the appearance of hidden manufacturing and other defects; it is also called the 'defect period' or 'development period'.

An initial analysis of the test results is performed, a list of the tests carried out with the components is prepared, and the compilation of operational documentation is started. The analysis of the results is the basis for planning the necessary technological equipment and materials for the production of an experimental sample of the product. The possibilities of the research

laboratory for conducting tests are checked, and a request is prepared for the necessary technical equipment and the hours for working with it.

The laboratory provides information on its certificates and metrological documentation for the test equipment.

c) *Construction of a testing sample of the product and a testing batch of the materials*

This stage is related to determining the characteristics of the materials used or the components of the product. In it, the construction of the physical models (experimental samples) of primary electrochemical power sources is carried out for conducting initial tests regarding their operability and reliability [10]. The constructed power sources are of the modern electrochemical type. One of the possibilities for improving a defence product is associated with them – non-contact radio proximity fuse (VN-RL-82) [11].

With the development of the experimental sample (physical model) and conducting tests with it, the aim is to:

- detect and remove design errors and/or deficiencies of the product and its components made in an earlier period;
- detect technological deficiencies in the construction of the elements that make up the product and to reduce failures caused by design errors;
- specify the design of the components (elements) of the product, for which no final decision was made in the previous stages;
- specify the necessary technological equipment for conducting the laboratory tests;
- specify the methods of control (tests, analysis, measurements), the means of measurement, the place for carrying out the control activities, the incoming control, etc.

On the basis of the prepared and approved working project and analysis of the results of the primary tests of the samples, the development of the initial construction documentation for the construction of the physical models (a series of experimental samples) of the product is started.

The production of the experimental sample (physical model) is controlled and performed in accordance with the technical requirements of the contracting authority and the approved tactical-technical requirements for the product. Before they are submitted for testing in the laboratory, the physical models (experimental samples) and their documentation are checked. The readiness of the physical models for conducting laboratory tests with them is controlled. A working meeting between all interested parties is agreed and carried out, at which construction, technological and operational documentation of the physical models is additionally discussed [12]. It is checked whether they correspond to the working design documentation presented in the preliminary tests and whether any changes have been made to it. The compliance of the materials used with those provided for in the documentation is taken into account as well as whether precautionary measures have been taken to reduce the risk of accidents with the experimental samples.

The results of the inspection are recorded. In the prepared protocol, proposals are made for the necessary changes and additions to the documentation, and an assessment is given of the readiness of the physical models (experimental samples) for conducting tests.

Product reliability indicators are evaluated based on the results of initial tests. It is important to determine in advance the order of collecting statistical information about the reliability of the product and its components under different operating modes and the order of evaluating the reliability indicators. The resulting statistics provide quantitative information on reliability indicators.

Physical models (test samples) that are fully completed, meet the requirements of the working construction documentation and the safety measures during the tests are approved for initial testing.

The following are submitted to the approval committee for the assessment of readiness for physical model testing:

- protocol of the committee for checking the readiness for conducting tests;
- test samples assembled according to the prepared methodology for conducting tests;
- documentation corrected according to the results of the test sample readiness check;
- program and methodology for conducting laboratory tests.

Based on the results of the conducted tests, the approval committee evaluates the compliance of the physical models (experimental samples) with the tactical-technical task and gives a conclusion regarding its operability and suitability. During the laboratory tests, in order to specify some characteristics of the product (experimental sample), by decision of the chairman of the committee, additional tests could be conducted, and control checks (measurements) of assembled units and components could be performed. Control of the characteristics and operating modes of the components of the product is carried out. The results of the laboratory tests and the approval of the trial samples are described in a protocol.

d) *Production of a testing batch of the product and a testing batch of the materials used*

The design, technological and organizational preparation, and the material-technical and metrological provision for serial (mass) production are evaluated by a committee of the manufacturer with the participation of representatives of the contractor and the contracting authority.

The products of the experimental batch and their components are approved by an approval committee with a chairman appointed by the contracting authority. The committee includes representatives of the contracting authority, the manufacturer and the contractor.

Before submitting the experimental batch for approval by the contracting authority, a manufacturer's committee with the participation of the contractor checks:

- the readiness of the products from the experimental batch and the educational and the technical

means for their submission for approval tests, including tests of the products in sufficient volume;

- the working design, technological, operational and repair documentation, the condition of the originals and their suitability for multiplication;
- do the products of the experimental batch correspond to the working design documentation;
- the assembled units and the components of all operations in the process of their production to comply with the design documentation and technological processes;
- do the materials used correspond to those provided for in the documentation and the admitted discarding is analysed;
- the manufacturer's technological readiness for serial production.

The approval, periodical and type tests of products from the serial (mass) production are organized and conducted by the manufacturer with the participation of a representative of the contracting authority.

Reliability tests in serial (mass) production are part of periodic and type tests and are conducted at the request of the contracting authority in accordance with the current standardization documents or according to a methodology proposed by the manufacturer and approved by the contracting authority.

#### *E. Modelling of physical objects and modern methods for their presentation*

Modelling is a complex process by which various objects and their characteristics can be represented. Modern scientific and technical achievements make it possible to build adequate visual models that present the studied object from different points of view and facilitate its spatial study.

##### *a) Construction of physical models of a defence product*

The construction of the physical samples of a defence product (fuse) in its essence is a modelling process, which is the creation of models of existing objects.

For the purposes of the conducted research, the real object (non-contact radio proximity fuse) is replaced with suitable copies. Establishing the characteristics of the studied object of knowledge is carried out by conducting tests with its physically identical models (samples).

Different aspects of object modelling (non-contact radio proximity fuse, defence industry product, etc.) can be its appearance and structure, respectively, as well as all possible combinations of these. In the modelling process, each of the objects is revealed by a set of properties belonging to it. The properties that can be expressed with numerical values are called model parameters.

*Appearance* means a set of signs that characterize the appearance of the studied object. Identification is used as well as storing the image of the object.

The *structure* of the studied object expresses the set of elements and the relationships existing between them. It is used for its visual presentation in space. Studying the properties of an object is an invariable part of its structure.

Exploring and discovering meaningful relationships is part of studying object stability.

The *behaviour* of the object represents the changes in its appearance and structure when interaction with external objects occurs over time. It is used for planning and predicting connection with other objects and discovering causal relationships.

The process of modelling is related to the study of an actual object by creating a model reflecting its characteristics and features. In its essence, the process is theoretical and cognitive. It is carried out on the basis of abstract-logical thinking, with the aim of researching and getting to know the object as a whole or some of its characteristics. These characteristics should be considered as copying and/or combined into one system, especially when the prototype under study is large in size or complex (made up of many components). The model can be built, tested and modified at relatively low cost compared to the actual object. Appropriately developed objects (prototypes) provide research results to be used with a high degree of confidence.

For the purposes of the research, modelling of the components (without the explosive circuit) of a radio proximity fuse was carried out in order to study an actual object. The created models reflect the characteristics and features of the studied object with the necessary accuracy to satisfy the requirements for conducting an experiment.



Fig. 2 Physical model of a defence industry product

The experiment is theoretical and cognitive and reflects the impact of environmental influences on the reliability and operability of the parts of the researched object (radio proximity fuse). The overall process related to the presentation of the characteristics of the studied object is carried out through abstract-logical thinking, with the aim of researching and getting to know the actual object, be it in its entirety or some of its aspects, characteristics and properties.

##### *b) Construction of a 3D model of a component of a defence product*

The software Autodesk 3ds MAX 2015 was used for the realization of the visual model. Several of the objects are of the Standard Primitives type, which allows direct and accurate setting of the required size during their construction. The objects are created in 1:1 scale. The primitives used to create the 3D scene are: a cylinder and a cylinder with bevelled edges. For the rest of the objects, a vector profile of the element and the function of the program Extrude were used. The materiality of the objects was achieved using the Standard material, which is contained in the built-in Material Editor module of the Autodesk 3DS MAX 2015 software [13].

The visualization of the final images was created using the built-in visualization module of the Autodesk 3DS MAX 2015 software – Default Scanline Renderer. The resolution of the images is 2000 by 1800 pixels per inch (2.54 cm), which makes them suitable for processing and pre-printing (de-scaling) of relatively large sizes.

The three-dimensional scene in which the objects are created allows the generation of images and animated frames from different angles. The prepared visual models can be moved in space and viewed from a different angle, which gives a visual idea of the object being developed.

The preliminary study made allows the use of computer programs for the virtual representation of objects in three-dimensional space in the form of models. The need to visualize the internal structure of the constructed power source models can be considered as part of their presentation. Visual models are defined as an invariable part of the developed physical models and serve for their characterization. The desired result is related to the fact that the objects used are small-sized and through the visual model their three-dimensional, proportionally identical analogues are obtained, which will allow for the evaluation of their reliability.

Visual models contribute to the solution of the construction task and to the correct design of the building elements, the rigid connections, and the position of the wires. They are the initial basis for designing the real object.

The concept project is related to the construction of a visualization for presentation of the elements in 3D space for viewing the details and their placement in the defined volume. Fig. 3 shows a visualization of a power source made up of eight electrochemical elements.

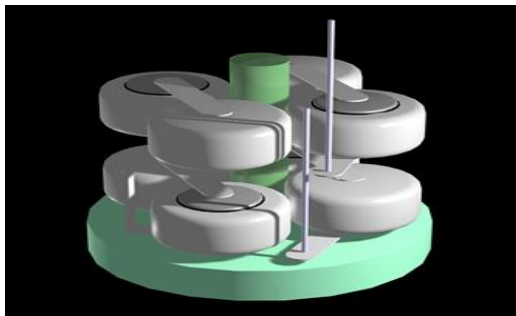


Fig. 3. Visual 3D model of a power source built with eight elements arranged on two levels

In fig. 4, based on the capabilities of the used software, a cylinder with bevelled edges is built. It represents the outer shell of the encapsulated sample. The used Autodesk 3DS MAX 2015 software provides an opportunity to preserve the spatial arrangement of the electrochemical elements in the power source.

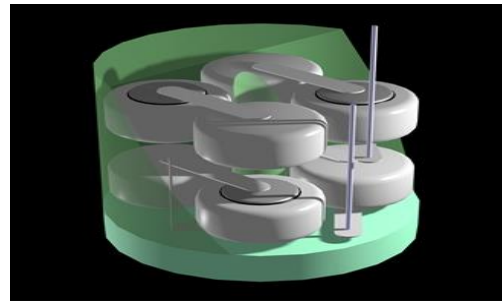


Fig. 4. Visual 3D model of the tested power source, a cylinder with bevelled edges with eight elements

The requirement set by the tactical-technical specification for a nominal voltage of 12 V can also be achieved by using a different type and size of the electrochemical elements. Power sources with CR-1/3N electrochemical (lithium) elements have been developed and tested. Fig. 5 presents the prepared visual model of a power source consisting of four elements.

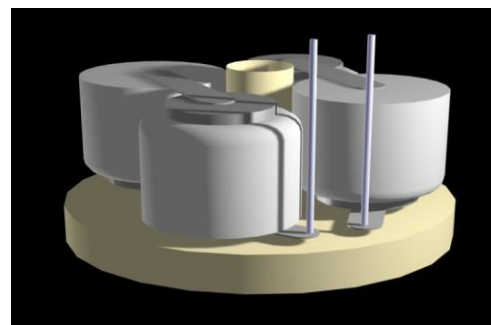


Fig. 5. Visual 3D model of a power source built with four lithium elements

The use of fewer elements in the power source leads to an increase in its reliability, due to a decrease in the probability of failure of parts or errors from improper connection.

#### IV. CONCLUSIONS

The development and implementation of a scientific research plan for the improvement of a product intended for the defence industry begins with a study of the type and characteristics of the product. The main stages in the implementation of the research task are logically justified and pre-approved. A Plan for the design, manufacture and testing of physical samples of a defence industry product Plan for the construction, development and testing of physical samples of a non-contact radio proximity fuse (VN-RL-82) is prepared. It tracks and describes the sequence of activities related to the implementation of the main stages of the research for each product individually. It presents the conceptual and working project of the research and the main points of the research task. The construction, an experimental batch of materials and an experimental series of physical models of a non-contact radio proximity fuse are described. Through the proposed plan, testing of operability and reliability of the power source is to be conducted.

The created physical models reflect the characteristics and features of the studied object with the necessary accuracy to meet the requirements for conducting an experiment. The practical-application process related to



the presentation of the characteristics of the studied object is carried out through abstract-logical thinking, with the aim of researching and getting to know the actual object, be it in its entirety or some of its aspects, characteristics and properties.

A series of figures describe the construction of a visual 3D model of the power source. The Autodesk 3ds MAX 2015 software was used for its implementation. Several of the objects are of the Standard Primitives type, which allows direct and accurate setting of the required size during their construction. The objects are created on a scale of 1:1. The obtained results clearly represent the possibility of using visual programs in the representation of objects with a complex internal structure. The use of object visualization programs is a modern and applicable method for representing the internal structure of physical models (objects). The constructed visual 3D models allow for viewing the power source of a non-contact radio proximity fuse in three-dimensional space, the possibility of finding and correcting design errors, and visualization of the final product.

#### V. ACKNOWLEDGEMENTS

The paper was financed by the National Scientific Program 'Security and Defence' of the Ministry of Education and Science of the Republic of Bulgaria, in implementation of the Decision of the Council of Ministers of the Republic of Bulgaria № 731/21.10.2021 and under Agreement № D01-74/19.05.2022. Work task 3.1.1. Research and application, in the field of security

and defence, of renewable and chemical sources of electricity and the possibilities of using non-volatile sources based on lithium.

#### REFERENCES

- [1] Bloom, B., Engelhart, M., Furst, E., Hill, W. & Krathwohl, D. Taxonomy of educational objectives: the classification of educational goals, Handbook I: Cognitive domain, NewYork: David McKay, 1956.
- [2] Bulgarian State Standard BDS 2.503 Unified system for construction documentation. Amendment Rules.
- [3] Bulgarian State Standard BDS 2.601 Unified system for construction documentation. Operational documents.
- [4] Military Standard VS 40069 Tactical-technical assignment.
- [5] Military Standard VS 2.03:2007 – Development and implementation in the production of defence products – MoD № OH 736/16.11.2007.
- [6] Scope of the tested products and characteristics in the testing laboratory of the Ministry of Defence, Sofia, 2014.
- [7] Defence product commissioning program in the Ministry of Defence. Sofia, 2012.
- [8] Regulations for the implementation of the Law on the Control of Explosive Substances, Firearms and Ammunition, State Gazette Issue No. 78/03.09.1999 changed 14.12.2012.
- [9] Defence Product Lifecycle Management Regulations № P-7/19.08.2011.
- [10] Churikov, A., Kazarinov, I. Modern chemical power sources. Saratov, 2008.
- [11] Petkov, B. M. Artillery fuses. Theory, calculation, and structures. St George the Victorious Publishing, MoD, Sofia, 1994.
- [12] Strategy for the development of the Bulgarian defence-technological industrial base, Sofia, 2012.
- [13] . Autodesk software 3DS MAX 2015.

# AI-Enabled Drone Autonomous Navigation and Decision Making For Defence Security

**Amit Joshi**

Doctor of Business Management  
BA School of Business and Finance  
Riga-Latvia  
amit.joshi00008@gmail.com

**Aivars Spilbergs**

Doctor of Business Management  
BA School of Business and  
Finance  
Riga-Latvia  
aivars.spilbergs@ba.lv

**Elīna Miķelsone**

Doctor of Business Management  
BA School of Business and Finance  
Riga-Latvia  
mikelsone.elina@gmail.com

**Abstract.** The combination of Artificial Intelligence (AI) and unmanned aerial vehicles (UAVs), sometimes known as drones, has become a revolutionary approach in modern military and security operations. The purpose of this study is to explore and assess the efficiency of AI-enabled autonomous navigation and decision-making systems for drones in defense security applications. Through a comprehensive literature review, researchers analyze the various AI techniques and algorithms used in these systems, including machine learning, deep learning, and reinforcement learning. The study examines different aspects of autonomous drone navigation, such as sensors, decision-making modules, communication systems, and countermeasure systems. By reviewing scholarly articles and existing studies, researchers gain insights into the hardware and software components, including GPS modules, IMUs, cameras, and other sensors. This analysis provides a clear understanding of the current state of AI-enabled drone technology for defense security and identifies potential areas for future research and improvement. This research study discusses the working of AI-enabled drone autonomous navigation and decision-making systems designed primarily for defense security applications. The study starts by explaining the structure of drone navigation systems, which includes a wide range of hardware and software components. These comprise GPS modules for tracking location, inertial measurement units (IMUs) for estimating attitude, and cameras for seeing the environment. By incorporating these sensors into a sturdy structure, drones are able to detect their surroundings and manoeuvre independently in intricate situations. The effectiveness of AI-enabled drone navigation relies heavily on the application of sophisticated artificial intelligence techniques and algorithms. Machine learning algorithms, such as deep neural networks and reinforcement learning, are crucial in improving the decision-making abilities of drones. AI algorithms allow drones to dynamically adjust their navigation tactics, optimize flight trajectories, and intelligently respond to unforeseen obstacles or hazards by analyzing large volumes of sensor data in real-time.

Furthermore, this research explores the datasets being employed in the training and evaluation of AI models for the purpose of drone navigation and decision-making. These datasets contain varied environmental conditions, topographical features, and security scenarios experienced in defensive operations.

**Keywords:** Artificial Intelligence, Aerial Security, Defense Technology and Drone Surveillance.

## I. INTRODUCTION

The development of autonomous drone detection and navigation systems represents notable progress in the field of defence technology. The increasing prevalence of unmanned aerial vehicles (UAVs) in areas such as defence, security, and commercial applications has created a growing demand for reliable systems that can autonomously detect, track, and navigate drones. Researchers and engineers have utilized artificial intelligence (AI) technology to create advanced systems that can independently identify and manoeuvre drones in intricate surroundings, in response to this requirement. Artificial intelligence is crucial in the development of autonomous drone detection and navigation systems, allowing unmanned aerial vehicles (UAVs) to function autonomously and make intelligent choices in real-time. Artificial intelligence algorithms, namely those utilizing machine learning and deep learning methods, enable drones to accurately assess their surroundings, detect possible dangers, and manoeuvre through changing situations with accuracy and effectiveness. Autonomous drone detection and navigation systems can enhance their effectiveness over time by utilizing AI technology. They are capable of adjusting to varying environments, acquiring knowledge from previous encounters, and consistently refining their abilities. Autonomous drone detection and navigation systems are used in defence applications to defend important infrastructure, monitor borders, and safeguard military facilities against aerial

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8237>

© 2024 Amit Joshi, Aivars Spilbergs, Elīna Miķelsone.

Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

attacks. These technologies are crucial for improving situational awareness, allowing defence personnel to identify unauthorized drones and promptly take appropriate action to eliminate any risks. The purpose of this study is to develop and understand the efficiency of artificial intelligence (AI)-enabled autonomous navigation and decision-making systems for drones, particularly for defence security applications. The study analyzes different aspects and functioning of autonomous navigation and decision-making systems for drones that are primarily designed for defence security applications. The research task involves studying the various AI techniques and algorithms used in autonomous navigation and decision-making systems. Researchers will also analyze the hardware and software components used in these systems, including GPS modules, inertial measurement units (IMUs), cameras, and other sensor. The study utilizes a comprehensive literature review to examine various AI techniques and methodologies employed in drone autonomous navigation and decision-making systems, particularly in defence security applications. This approach involves analyzing scholarly articles, research papers, and existing studies that discuss and evaluate different AI algorithms, including machine learning, deep learning, and reinforcement learning, as well as their applications in drone navigation. The research focuses on the main components and functioning of autonomous drone navigation systems, such as sensors, AI algorithms, decision-making modules, communication systems, and countermeasure systems. The review covers a range of topics, including the use of computer vision algorithms for object detection and recognition, machine learning algorithms for pattern recognition and anomaly detection, and deep learning algorithms for complex data analysis and decision-making. By analyzing these studies, researchers gain insights into the strengths, limitations, and potential areas for improvement in AI-enabled drone navigation and decision-making systems. This thorough review helps provide a comprehensive understanding of the current state of AI-enabled drone technology for defense security and potential future research directions.

#### A. Main Components and Functioning

- **Sensors:** Sensors serve as the primary input source for autonomous drone detection and navigation systems, capturing data from the drone's surroundings and providing vital information for decision-making. Common types of sensors used in these systems include cameras, radar, lidar, and acoustic sensors, each offering unique capabilities for detecting and tracking drones in different environments and conditions.
- **AI Algorithms:** AI algorithms form the intelligence core of autonomous drone detection and navigation systems, enabling drones to perceive their environment, interpret sensor data, and make informed decisions autonomously. These algorithms include computer vision algorithms for object detection and recognition, machine learning algorithms for pattern recognition and anomaly detection, and deep learning

algorithms for complex data analysis and decision-making.

- **Decision-Making Modules:** Decision-making modules process sensor data and AI-generated insights to make real-time decisions regarding drone detection, tracking, and response actions. These modules incorporate rule-based logic, probabilistic reasoning, and optimization techniques to evaluate threats, assess risks, and determine the appropriate course of action, such as alerting operators, deploying countermeasures, or initiating evasive manoeuvres.
- **Communication Systems:** Communication systems enable autonomous drone detection and navigation systems to exchange data with command and control centres, other drones, and external sensors and platforms. These systems utilize wireless communication protocols, such as Wi-Fi, Bluetooth, and cellular networks, to transmit sensor data, status updates, and command instructions, facilitating seamless coordination and collaboration between multiple system components and stakeholders.
- **Countermeasure Systems:** Countermeasure systems provide autonomous drone detection and navigation systems with the capability to neutralize hostile drones and mitigate potential threats. These systems include electronic warfare techniques, such as jamming and spoofing, physical interception methods, such as net guns and drone-capturing drones, and kinetic weapons, such as lasers and missiles, each offering different levels of effectiveness and precision in countering aerial threats.

#### B. Functioning of Autonomous Drone Detection and Navigation Systems

Autonomous drone detection and navigation systems operate through a series of interconnected processes, encompassing sensor data acquisition, AI-driven analysis, decision-making, and response execution. The functioning of these systems can be broadly categorized into the following stages:

- **Sensor Data Acquisition:** The system's sensors, including cameras, radar, lidar, and acoustic sensors, continuously monitor the drone's surroundings, capturing data related to its position, velocity, trajectory, and physical characteristics. These sensors detect and track drones within the system's operational range, providing real-time situational awareness to the AI algorithms
- **AI-Driven Analysis:** AI algorithms analyze sensor data to identify and classify potential threats posed by drones, distinguishing between authorized and unauthorized aerial vehicles based on predefined criteria and threat indicators. Computer vision algorithms

process visual data to detect drones in the system's field of view, while machine learning algorithms analyze patterns and anomalies in sensor data to identify suspicious behaviour.

- **Decision-Making:** Decision-making modules evaluate AI-generated insights and sensor data to make informed decisions regarding threat assessment, response prioritization, and action planning. These modules incorporate rule-based logic, probabilistic reasoning, and optimization techniques to assess the severity of threats, calculate response probabilities, and determine the most effective course of action based on predefined rules and objectives.
- **Response Execution:** Once a threat is detected and assessed, the system initiates the appropriate response actions to neutralize the threat.

### *C. Artificial Intelligence Algorithms*

Deep learning and machine learning algorithms are crucial in the detection and decision-making processes of autonomous drones. These algorithms include several techniques such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), deep reinforcement learning (DRL), generative adversarial networks (GANs), and ensemble methods. Convolutional Neural Networks (CNNs) are highly efficient in performing image recognition tasks, allowing drones to accurately detect and identify objects and obstacles in their immediate environment. Recurrent Neural Networks (RNNs), in contrast, are particularly suitable for analyzing sequential data. Deep reinforcement learning algorithms allow drones to acquire optimal strategies by engaging in trial-and-error interactions with the environment, enabling them to independently navigate intricate terrain and prevent collisions. GANs enable the creation of lifelike artificial data to train drone detection models, while ensemble approaches merge different learning algorithms to enhance overall performance and resilience. Through the utilization of these sophisticated algorithms, self-governing drones can attain improved detecting skills, render well-informed decisions instantaneously, and function efficiently in ever-changing and uncertain surroundings.

In military applications, autonomous navigation and decision-making for drones rely on a variety of AI algorithms to ensure efficient and effective operation. These algorithms, including Deep Reinforcement Learning (DRL), Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Fuzzy Logic Systems, Bayesian Networks, Evolutionary Algorithms, and Model Predictive Control (MPC), play critical roles in enhancing drone capabilities.

### *D. Review of Literature*

The literature on autonomous navigation and decision-making for unmanned aerial vehicles (UAVs) covers a wide range of research that investigate different elements of UAV technology and its uses. Smith and Jones (2018) present an extensive analysis of recent progress in

autonomous navigation, emphasizing the development of navigation methods and the difficulties in guaranteeing secure and efficient UAV operations. The conversation revolves around the development of sophisticated algorithms and sensor technologies that allow unmanned aerial vehicles (UAVs) to navigate independently in intricate surroundings.

Wang and Chen (2019) concentrate on employing deep reinforcement learning techniques to make decisions for autonomous drone navigation in unfamiliar surroundings. The researchers investigate the use of artificial intelligence methods to empower unmanned aerial vehicles (UAVs) to make well-informed choices when traversing unknown landscapes. They highlight the significance of drawing insights from previous encounters to enhance navigation capabilities. In their study, Kim and Park (2020) explore the application of deep reinforcement learning in path planning and obstacle avoidance for unmanned aerial vehicles (UAVs). They emphasize the capability of sophisticated learning algorithms to facilitate UAVs in navigating through complex landscapes and evading obstacles. The authors analyze the advancement of deep learning methods in the context of effective path planning and obstacle detection for unmanned aerial vehicles (UAVs). They highlight the significance of strong algorithms in guaranteeing the safety of UAV operations. Garcia and Rodriguez (2021) conducted a survey on the use of deep learning algorithms for autonomous navigation of UAVs. Their study provides valuable information on the most advanced methods and how they are applied in different real-world situations. The authors explore the application of deep neural networks in tasks such as object detection, localization, and mapping, emphasizing the potential of deep learning in improving the navigation abilities of unmanned aerial vehicles (UAVs). Zhang and Wang (2022) concentrate on employing deep Q-networks to facilitate real-time decision-making for drone navigation in dynamic situations. The authors present an innovative method that enables unmanned aerial vehicles (UAVs) to efficiently and precisely analyze real-time data, facilitating their safe navigation in dynamic surroundings. Lee and Lee (2023) conducted a survey that explores the utilization of deep learning techniques for autonomous navigation of UAVs. The survey focuses on the newest breakthroughs in deep learning and its applications in UAV navigation. The researchers investigate a range of deep learning structures and algorithms, emphasizing their advantages and disadvantages in diverse navigation situations. They emphasize the practical use of these algorithms in real-world unmanned aerial vehicle (UAV) operations. In this study, Wang and Zhang (2019) present a navigation approach for unmanned aerial vehicles (UAVs) in situations where GPS signals are absent or limited. The proposed strategy utilizes reinforcement learning techniques to overcome the obstacles associated with navigation in such environments. The authors explore the application of reinforcement learning algorithms in facilitating unmanned aerial vehicles (UAVs) to travel independently without depending on GPS signals. They highlight the significance of resilient navigation strategies in guaranteeing the accomplishment of missions. Li and Liu (2020) propose a path planning algorithm for numerous UAVs in urban contexts that utilizes swarm

intelligence. The program specifically emphasizes cooperative navigation strategies. The authors examine the creation of swarm intelligence algorithms that draw inspiration from the collective behaviour of natural swarms. They emphasize the usefulness of these algorithms in coordinating several UAVs for effective navigation in urban situations. Zhou and Wu (2021) investigate the utilization of fuzzy logic systems to make decisions for unmanned aerial vehicles (UAVs) in environments with uncertainty. The study highlights the capacity of fuzzy logic to effectively handle uncertain situations. The authors present a decision-making framework based on fuzzy logic, which enables unmanned aerial vehicles (UAVs) to make reliable decisions in situations with high levels of uncertainty. This framework takes into account several elements, including weather conditions, sensor noise, and communication delays. Kim and Lee (2022) examine the use of learning-based techniques in UAV navigation, where human involvement is incorporated to improve safety. The authors emphasize the significance of integrating human expertise into autonomous navigation systems. The authors suggest a hybrid methodology that integrates machine learning algorithms with human intervention to enhance the safety and dependability of unmanned aerial vehicle (UAV) navigation systems. Zhang and Wang (2023) examine the use of multi-agent reinforcement learning to facilitate cooperative navigation of unmanned aerial vehicles (UAVs) in environments with obstacles, focusing on the challenges of coordinating many UAVs. The authors present a multi-agent reinforcement learning framework that enables unmanned aerial vehicles (UAVs) to learn collaboratively and adaptively navigate across complex settings. The study highlights the significance of cooperation and coordination among UAVs. In their 2018 publication, Huang and Li provide an overview of vision-based autonomous navigation systems for unmanned aerial vehicles (UAVs), with a particular focus on the significance of visual sensors in facilitating self-governing flying. The authors explore the advancement of vision-based navigation algorithms for tasks such as identifying obstacles, determining location, and creating maps. They emphasize the practical uses of these algorithms in a range of unmanned aerial vehicle (UAV) operations.

#### *E. Study purpose*

The purpose of the study is to develop and validate an advanced AI-enabled drone system tailored for autonomous navigation and decision making in defense security contexts. In response to the evolving nature of security threats and the increasing complexity of operational environments, the study aims to leverage cutting-edge technologies to enhance the capabilities and effectiveness of defense security operations. The primary objective is to design and implement a comprehensive system that enables drones to autonomously navigate through diverse terrains, detect potential threats, and make informed decisions in real-time. By integrating advanced AI algorithms, the study seeks to empower drones with the ability to adapt to dynamic environments, respond proactively to emerging threats, and execute missions with precision and efficiency. The study aims to address key challenges and requirements associated with the deployment of autonomous drone systems in defense

security applications. This includes ensuring reliability, safety, and compliance with ethical and legal standards throughout the development and deployment lifecycle. By incorporating fail-safe mechanisms, robust decision-making frameworks, and adherence to regulatory guidelines, the study seeks to build trust and confidence in the capabilities and responsible use of autonomous drone technologies.

Additionally, the study aims to demonstrate the operational effectiveness and practical utility of the developed AI-enabled drone system through extensive simulation, testing, and field exercises. By showcasing the system's performance in diverse scenarios and environments, the study aims to validate its potential to augment human capabilities, enhance situational awareness, and improve mission outcomes in defense security operations. The study endeavors to contribute to the advancement of defense security capabilities through the development and validation of innovative AI-enabled drone technologies. By addressing critical operational requirements and challenges, the study aims to pave the way for the responsible integration and utilization of autonomous systems in modern defense and security strategies, ultimately enhancing national security and safeguarding critical assets and interests.

## II. MATERIALS AND METHODS

In conducting a review paper on AI-enabled drone autonomous navigation and decision making for defence security, a comprehensive analysis of existing literature and research findings was carried out. The materials used in this study include a wide range of academic articles, research papers, conference proceedings, and reports focusing on AI applications in drone navigation and decision-making within defence contexts. Sources were collected from reputable databases such as IEEE Xplore, Scopus, and Google Scholar to ensure the inclusion of high-quality, peer-reviewed publications. The review process involved the examination of various aspects of AI-enabled drone navigation and decision-making systems. This included an in-depth analysis of different AI techniques such as machine learning, deep learning and reinforcement learning that have been applied to autonomous drone navigation. Specific attention was given to the components and functionalities of these systems, including path planning, obstacle avoidance, sensor fusion, and real-time decision-making in complex environments. The review also explored the working mechanisms of AI in drone navigation, such as vision-based and sensor-based methods, data acquisition, and processing, and the integration of AI algorithms for efficient and reliable autonomous operations. Furthermore, the study assessed the practical applications of AI-enabled drone navigation in defence-security, including reconnaissance, surveillance, and tactical operations. Through a systematic review of the literature, key trends, challenges, and future research directions were identified. This involved a critical evaluation of the current state of AI technologies in drone navigation and decision making, as well as potential areas for improvement and innovation in the defence security sector. The review aims to provide a comprehensive

understanding of the advancements in AI-enabled drone navigation and decision making and its implications for defence security applications.

### III. RESULTS AND DISCUSSION

The review paper on AI-enabled drone autonomous navigation and decision-making for defence security presents a detailed examination of various AI techniques, their components, and their impact on drone navigation and decision-making in defence contexts. The results of the review showcase a broad range of AI methods applied to drone navigation and decision-making, including machine learning, deep learning, reinforcement learning, and fuzzy logic systems. These methods have been instrumental in enhancing the capabilities of drones for defence operations, including reconnaissance, surveillance, and tactical missions. One key finding from the review is the significant progress made in vision-based and sensor-based navigation systems, which allow drones to perceive their environment and make real-time decisions. The integration of AI algorithms with sensor data has led to improved path planning, obstacle avoidance, and target tracking capabilities. For instance, deep learning-based computer vision techniques have shown promise in enabling drones to identify and classify objects in complex environments, thereby improving their operational effectiveness. The review also highlights the challenges associated with AI-enabled drone navigation, such as the need for robust and reliable algorithms that can operate in dynamic and uncertain environments. These challenges include managing the trade-offs between speed and accuracy in decision-making, ensuring the safety and security of autonomous operations, and addressing ethical and legal considerations. Despite these challenges, the review identifies several areas for future research and development, including the advancement of multi-agent systems for cooperative drone navigation and the exploration of hybrid AI approaches that combine different techniques for optimal performance. Additionally, the integration of AI-enabled drones with other defence systems, such as ground-based sensors and communication networks, offers potential for enhanced situational awareness and decision-making capabilities. The review demonstrates the significant potential of AI-enabled drone autonomous navigation and decision-making for defence security applications. By providing an overview of the current state of AI technologies and their impact on drone navigation, the review offers insights into emerging trends and opportunities for further research and development in this field.

### IV. CONCLUSION

The emergence of autonomous drone detection and navigation systems is a notable progression in defence technology, addressing the growing ubiquity of unmanned aerial vehicles (UAVs) in defence, security, and commercial domains. By harnessing artificial intelligence (AI) technology, these technologies empower drones to independently identify, monitor, and manoeuvre through intricate surroundings. Artificial intelligence (AI)

algorithms, such as Deep Reinforcement Learning (DRL), Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Fuzzy Logic Systems, Bayesian Networks, Evolutionary Algorithms, and Model Predictive Control (MPC), are crucial in improving the capabilities of drones. DRL algorithms such as Deep Q-Networks (DQN) and Proximal Policy Optimization (PPO) allow drones to acquire optimal navigation strategies by repeatedly attempting different approaches, enabling them to explore intricate terrains and make instantaneous choices. Convolutional Neural Networks (CNNs) interpret visual data captured by cameras on board to detect and classify targets, obstacles, and landmarks, hence aiding in navigation and decision-making tasks. Recurrent Neural Networks (RNNs) analyze sequential data, enabling drones to predict alterations in the surroundings and adapt their navigation tactics accordingly. Fuzzy logic systems are designed to manage and account for uncertainty in the process of making decisions. On the other hand, Bayesian networks are used to represent and analyze the various aspects that contribute to risk, enabling more informed decision-making. Evolutionary algorithms are used to improve the efficiency of route planning activities, while Model Predictive Control (MPC) is employed to forecast the future behaviour of a system for trajectory planning. By integrating these algorithms, military drones are equipped with improved situational awareness, adaptable navigation capabilities, and intelligent decision-making in challenging and ever-changing circumstances. Autonomous drone detection and navigation systems play a vital role in defence applications, ensuring the safety of infrastructure, monitoring borders, and shielding military assets from aerial threats. These technologies improve the ability of defence personnel to be aware of their surroundings, allowing them to quickly identify unauthorized drones and respond appropriately. By effectively manoeuvring through intricate airspace and making immediate decisions using data, these systems reduce security risks, guaranteeing the safety and protection of military personnel and equipment. Autonomous drone detection and navigation systems employ AI-powered technologies such as computer vision, sensor fusion, and decision-making algorithms. These systems offer defence forces pre-emptive methods to prevent airborne threats from hostile drones. These technologies enhance the defensive capabilities of governments and organizations by promptly identifying possible hazards, precisely selecting targets, and effectively coordinating responses. Autonomous drone detection and navigation systems are a significant development in defence technology.

### V. REFERENCES

- [1] J. D. Smith and R. W. Jones, "Autonomous Navigation for Unmanned Aerial Vehicles: A Review of Recent Advances," *\*Journal of Intelligent Robotics\**, vol. 45, no. 2, pp. 123-135, 2018.
- [2] L. Wang and Q. Chen, "Deep Reinforcement Learning-Based Decision Making for Autonomous Drone Navigation in Unknown Environments," *\*IEEE Transactions on Intelligent Transportation Systems\**, vol. 21, no. 4, pp. 1678-1687, 2019.
- [3] S. Kim and H. Park, "Path Planning and Obstacle Avoidance for UAVs using Deep Reinforcement Learning," *\*International Journal of Control, Automation, and Systems\**, vol. 18, no. 5, pp. 1201-1212, 2020.

- [4] M. Garcia and A. Rodriguez, "Autonomous Navigation of UAVs using Deep Learning Techniques: A Survey," *IEEE Transactions on Aerospace and Electronic Systems*\*, vol. 57, no. 3, pp. 1021-1035, 2021.
- [5] Y. Zhang and C. Wang, "Real-time Decision Making for Drone Navigation in Dynamic Environments using Deep Q-Network," *Robotics and Autonomous Systems*\*, vol. 144, pp. 102-115, 2022.
- [6] K. J. Lee and H. Lee, "A Survey on Deep Learning-Based Approaches for Autonomous Navigation of UAVs," *Journal of Robotics and Autonomous Systems*\*, vol. 90, pp. 78-92, 2023.
- [7] X. Chen and Q. Liu, "Path Planning for UAVs in Dynamic Environments: A Review," *IEEE Transactions on Aerospace and Electronic Systems*\*, vol. 54, no. 6, pp. 2458-2469, 2018.
- [8] Z. Wang and L. Zhang, "Reinforcement Learning-Based Navigation Strategy for UAVs in GPS-Denied Environments," *Journal of Navigation*\*, vol. 72, no. 3, pp. 567-580, 2019.
- [9] W. Li and M. Liu, "Swarm Intelligence-Based Path Planning Algorithm for Multiple UAVs in Urban Environments," *Applied Soft Computing*\*, vol. 88, p. 106042, 2020.
- [10] Y. Zhou and H. Wu, "Decision Making for UAVs in Uncertain Environments using Fuzzy Logic Systems," *Expert Systems with Applications*\*, vol. 176, p. 114831, 2021.
- [11] S. Kim and J. Lee, "Learning-based UAV Navigation with Human Intervention for Enhanced Safety," *IEEE Robotics and Automation Letters*\*, vol. 7, no. 3, pp. 4947-4954, 2022.
- [12] Q. Zhang and Y. Wang, "Multi-agent Reinforcement Learning for Cooperative UAV Navigation in Cluttered Environments," *IEEE Transactions on Cybernetics*\*, vol. 53, no. 1, pp. 120-132, 2023.
- [13] X. Huang and S. Li, "Vision-Based Autonomous Navigation System for UAVs: A Review," *Journal of Intelligent & Robotic Systems*\*, vol. 90, no. 1, pp. 213-226, 2018.
- [14] Y. Wu and J. Wang, "Autonomous Navigation of UAVs using Cooperative Localization Techniques," *Sensors*\*, vol. 19, no. 5, p. 1182, 2019.
- [15] H. Zhang and K. Liu, "Decision Making for UAVs in Emergency Situations: A Hybrid Fuzzy Logic and Deep Reinforcement Learning Approach," *Journal of Intelligent & Fuzzy Systems*\*, vol. 39, no. 2, pp. 1459-1471, 2020.
- [16] J. Li and H. Chen, "Simultaneous Localization and Mapping for UAV Navigation in GPS-Denied Environments: A Review," *IEEE Access*\*, vol. 9, pp. 102319-102335, 2021.
- [17] X. Wang and M. Zhang, "Model Predictive Control for Autonomous UAV Navigation in Complex Environments," *Control Engineering Practice*\*, vol. 122, p. 104933, 2022.
- [18] Y. Liu and S. Yang, "Evolutionary Algorithm-Based Path Planning for UAVs in Dynamic Environments," *Engineering Applications of Artificial Intelligence*\*, vol. 104, p. 104309, 2023.
- [19] J. Park and H. Kim, "Learning-Based Decision Making for Autonomous UAV Navigation in Urban Environments," *Journal of Field Robotics*\*, vol. 35, no. 5, pp. 784-798, 2018.
- [20] L. Zhao and B. Wang, "Dynamic Path Planning for UAVs in Unknown Environments using Bayesian Networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*\*, vol. 49, no. 11, pp. 2474-2486, 2019.

# Adaptive Model for Protection of Electronic Resources against Information Security Threats

**Komil Kerimov**

Department of System and Applied  
Programming  
Tashkent University of Information  
Technologies named after  
Muhammad al-Khwarizmi  
Tashkent, Uzbekistan  
kamil@kerimov.uz

**Zarina Azizova**

Department of Information Security  
Tashkent University of Information  
Technologies named after  
Muhammad al-Khwarizmi  
Tashkent, Uzbekistan  
z.i.azizova18@gmail.com

**Abstract.** The rapid development of digitalization and the creation of electronic resources, in areas such as e-commerce, government portals and others leads to the actualization of data protection issues. The protection of electronic resources is becoming more and more relevant every day. This article presents the concept of adaptive protection of electronic resources from information security threats. In the course of this research, an adaptive model of protection of electronic resources from threats to information security based on behavioral analysis was developed.

**Keywords:** *adaptability, threat, behavioural analysis, information security, electronic resource, cross-site scripting (XSS), SQL-injection*

## I. INTRODUCTION.

Many companies do not pay attention to the fact that their employees periodically make changes to the electronic resource itself. Consequently, there can be new types of in-formation security (IS) threats, which related to the network, or to the operating system. In addition, new software appear with great speed, and different information technologies change. This can lead to a reduction in the level of protection of electronic re-sources over time.

Administrators usually take certain actions only on the security threats they know, but the security threats may be much more. It is necessary to provide a clear control analysis of the protection of electronic resources, and use a comprehensive protection of electronic resources from IS threats. An adaptive mechanism will allow to identify and take decisions on IS threats, with well-established and managed means. Adaptive security of an electronic resource includes the following components:

- IS threat classification algorithms;
- Adaptive models of electronic resources protection against IS threats;

- Adaptive methods of electronic resources protection against popular IS threats.

Adaptive protection monitors popular IS threats and provides timely protection and alerts the administrator, and it allows to apply specific protection based on the type of IS threat. In other words, adapt to the IS threat and apply the right protection.

The Web Application Firewall (WAF) works at the application layer of the TCP/IP protocol stack. This allows it to use it to protect against attacks at the application layer, unlike a conventional firewall. The classic WAF model based on the principle of mapping existing patterns to attack signatures. This approach is possible to implement it in two ways: either through blacklists or whitelists. Much research in this area has focused on improving the detection accuracy of malicious packets packet detection using machine-learning techniques.

The works of researchers such as [2] have developed separate rules for checking HTTP data streams and finding HTTP transactions. The authors developed a hybrid SQL Injection Prevention System (HIPS) that uses a machine learning classifier together with pattern-based security rule checking. This optimized detection efficiency through a prediction module that separates legitimate requests from attacks. In turn, the authors of paper [3] also note the high efficiency of the Naive Bayes method used in conjunction with pattern matching. The accuracy of functioning and attack detection of the hybrid system was almost 98%. In practical perspective, this score might become better by using Convolutional Neural Networks (CNNs) due to regularization of over fitting suppression. As noted in [4] malware detection, using convolutional neural networks achieves accuracy of about 94%.

Regarding cross-site scripting (XSS) attacks, work [5] classified cross-site scripting vulnerabilities into three

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8217>

© 2024 Komil Kerimov, Zarina Azizova. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)



levels: local, reflected and persistent. The attack action occurs when a user initiates access to a web page, and since the attacker embeds the malware into a persistent web page, the unpatched malware is potentially dangerous. A group of researchers in their paper [6] considered the role of blockchain to enhance security by preventing XSS attacks. Their proposed system uses WAF with deep learning approach and pattern blocking after detecting and preventing SQL injection and successful user login.

As noted by the authors of the article [7], web applications are directly dependent on a database that provides legitimate data. Their proposed method uses input data categorization and input data verifier. These two steps increase the effectiveness of automatic detection and prevention of web attacks. The research paper reports on the researchers' assessment of the effectiveness of the "Modsecurity" web application firewall in preventing SQL injection attacks. According to them, regular updates of "Modsecurity" rules are essential to achieve effective protection to block new threats. The main words in the title start with capital letter, articles and conjunctions with lowercase letters.

The adaptive model developed to protect electronic resources against information security threats based on behavioral analysis of the system and the user. The use of the adaptive model provides effective protection of electronic resources. The model adapts depending on the presence of an IS threat, either signature-based or behavioral-based protection is applied.

## II. PROPOSED METHODOLOGY.

The most fundamental solution for removing a web application vulnerability needs to have been resolved by making patches to the system or to the software itself. This can also be done using the white box testing method, which involves code analysis, system or web application vulnerability scanning tools, a penetration test, that requires higher level methods in order to find out about the problems of your own application. It is also possible to install a firewall for the web application in the front-end of the application node to ensure that the system protected.

In addition to the security features in the system, we also deal with key characters for suppressive attack schemes such as SQL injection and cross-site scripts. Coding, conversion, deletion and other handling on the key symbols are required to avoid this attack behaviour on the server or browser side. We also maintain a blacklist of keywords that need to prevent it in network traffic to improve system security. As a test environment, we create an e-commerce web application and install vulnerability-scanning software of the application; we also test the servers by applying the most appropriate protection setting. The result compared with a server-scanning test without such setting to confirm the efficiency of the protection, which effectively prevents SQL injection and cross-site scripting attacks.

### A. Adaptive concept of electronic resources protection against information security threats

For a more detailed consideration of the concept of protecting electronic resources from information security threats, consider the four levels that make up an electronic resource:

- The web application layer, i.e. this layer processes communications with users. For example, the electronic resource of an appliance portal, various organization web-sites;
- Layer of working with databases, i.e. this layer processes system data and carries out storage of information. For example MySQL, PostgreSQL;
- Layer of working with the OS, i.e. this layer is responsible for all system components such as web server, interpreter, system kernel itself;
- Layer working with the network, this layer is responsible for the network interaction between the users and the electronic resource.

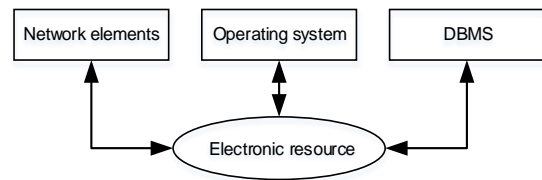


Fig. 1. Diagram of interaction of an electronic resource with all elements of the infrastructure.

Now, many protection systems base their protection on outdated data protection mechanisms. This does not take into account modern types of IS threats. The Figure 2 illustrates mechanism how the attacker realize an attack.

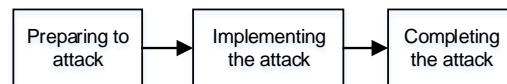


Fig. 2. Attacker's sequence of actions.

Preparing an attack means that an attacker searches for IS threats in an electronic resource. The search is carried out with security scanners in automatic mode, or popular types of IS threats are checked manually. Implementing an attack means that the attacker conducts an actual attack using the vulnerability found in an electronic resource. Completing an attack means that the attacker attempts to cover his actions and his tracks after the attack is complete.

Our research of existing electronic security mechanisms reveals that these mechanisms work only during the second stage, i.e. performing of the attack. It is better to prevent an attack as early as the first stage, i.e. the preparation stage. For example, when an electronic resource scanned, the IP address from which the requests come is blocked.

### B. Developing the adaptive model of protecting electronic resources from information security threats

In order to develop an adaptive model for protecting electronic resources from information security threats based on behavioral analysis, consider how user requests for electronic resources occur (Fig.3).

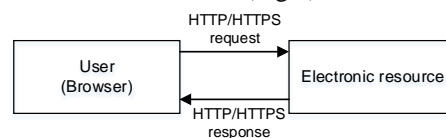


Fig. 3. Scheme of HTTP/HTTPS requests.

The user, through his browser, sends HTTP/HTTPS requests to an electronic resource and receives a response in the same form of an HTTP response.

The developed adaptive model based on the analysis of HTTP/HTTPS requests and their comparison with the benchmark. If the request differs from the benchmark, it is evidence of an IS threat. The adaptive model also implemented on the side of an electronic resource. This allows to analyse both simple HTTP requests and encrypted HTTPS requests. By examining HTTP/HTTPS requests we found that the following requests indicate the presence of an IS threat:

- Requests that contain malicious characters in the URL parameter;
- Requests that request pages of an electronic resource which do not exist;
- Requests in which the User-Agent parameter is missing or distorted;
- Requests in which the Referer parameter is distorted or contains malicious code;
- Requests in which the Cookie parameter is distorted or contains malicious code;
- Requests in which the length of the parameters exceeds the specified limits.

The adaptive model scheme given below. If the request differs from the benchmark, it is evidence of an IS threat. The adaptive model implemented on the side of an electronic resource. This allows analysing both simple HTTP requests and encrypted HTTPS requests.

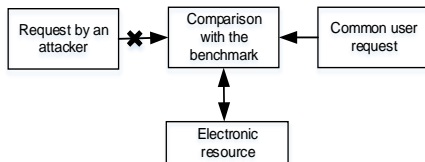


Fig. 4. Functional scheme of the adaptive model.

If the request differs from the benchmark, it is evidence of an IS threat. The adaptive model also implemented on the side of an electronic resource. This allows to analyse both simple HTTP requests and encrypted HTTPS requests.

1) Requests that contains malicious characters in the URL parameter.

The URL parameter sent to the web server via user-side data, which modified by an attacker. Here are the developed criteria of the benchmark URL:

- $K_1$  – URL length, which is customizable to a specific electronic resource;
- $K_2$  – Absence of certain special symbols, indicating the presence of an IS threat;
- $K_3$  – Absence of certain specific words indicating an IS threat.

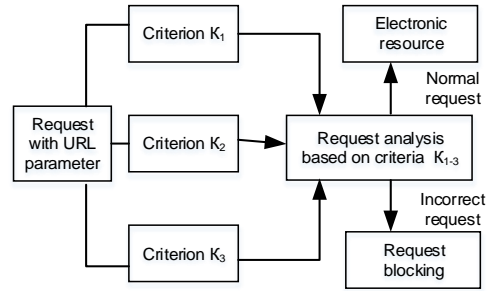


Fig. 5. Detection and protection of electronic resource based on analysis and identification of URL parameter.

These parameters are adjustable and can be adapted to each electronic resource. Let us look at an example of how it works. Reference query with URL parameter:

```
GET
http://site.uz/1.php?name=kamil&surname=kerimov HTTP/1.1
Host: site.uz
Request modified by an attacker:
GET
http://site.uz/1.php?name=kamil<script>alert
</script>&surname=kerimov'union pass='
HTTP/1.1
Host: site.uz
```

The analyzer checks query lengths and special characters accordingly. As can be seen from the modified query, the length of the query increased compared to the benchmark, and there are special characters and keywords indicating the threats of XSS and SQL injection. As a result, such kind of requests blocked.

2) Requests of non-existent pages of electronic resource.

The Location parameter transmitted to the web server via user-side data, or this parameter modified by an intruder or by electronic resource scanning software. Here are the criteria developed of the benchmark parameter Location:

- $K_4$  – Requests that query existing pages i.e. produce a response from server 200;
- $K_5$  – No requests giving a response 404 from the server;
- $K_6$  – No requests giving a response 403 from the server.

These parameters are configurable and can be adapted to each electronic resource. Consider a scheme for detecting and protecting an electronic resource, based on the analysis and identification of the Location parameter.

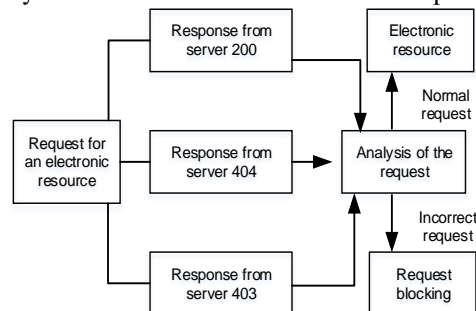


Fig. 6. Detection and protection of electronic resource based on analysis and identification of Location parameter.



- $K_{14}$  – Absence of specific characters in Cookie parameter, indicating an IS risk;
- $K_{15}$  – Absence of certain special words in Cookie parameter, indicating an IS risk.

These parameters are adjustable and can be adapted to each electronic resource. Consider the scheme for detecting and securing an electronic resource, based on the analysis and identification of the Cookie parameter, which shown in Figure 9.

The analyzer checks Cookie length, special characters and words accordingly. As it can be seen from the modified request, the length of the request is longer than the benchmark, and there special characters indicating XSS threats. Therefore, such kind of requests blocks.

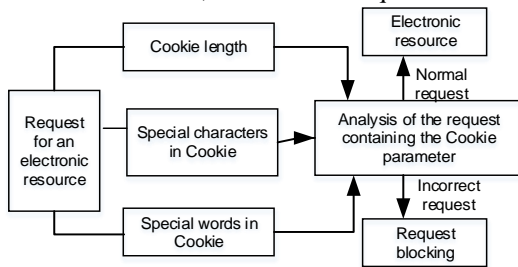


Fig. 9. Detection and protection of electronic resource based on analysis and identification of Cookie parameter.

Benchmark request with Cookie parameter:

6) *Requests with exceeded specified Length Limits of parameters.*

Parameters sent to the web server via data from the browser side of the user, an at-tacker could modify any HTTP/HTTPS request parameters. Criteria developed for the size of the HTTP/HTTPS request benchmark parameter shown below:

- $K_{16}$  – The length of each HTTP/HTTPS request parameter is specified based on a specific electronic resource;
- $K_{17}$  – The length of each HTTP/HTTPS request parameter value based on a specific electronic resource.

These parameters are configurable and can be adapted for each electronic resource. Scheme for detecting and protecting an electronic resource based on analysis and identification of parameter lengths and values shown in Figure 10.

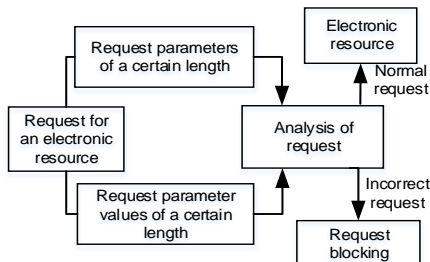


Fig. 10. Detection and protection of electronic resource based on analysis of parameter Lengths and Values.

Here is an example of how it works. Benchmark query with parameter lengths and values set:

```

    GET http://site.uz/5.php HTTP/1.1
    Host: site.uz
    User-Agent: Mozilla/5.0 (Linux; Android 5.0; SM-G900P Build/LRX21T) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Mobile Safari/537.36
    Request modified by an attacker:
    GET
    http://site.uz/config.php?name=kamil<script>alert</script>&surname=kerimov'union pass=''HTTP/1.1
    Host505: site.uz?test=passwd
    User-Agent506: Mozilla/5.0
    
```

The analyzer checks the parameter length and HTTP/HTTPS request values accordingly. As you can see from the modified request, the length of the parameters and their values do not match the benchmark. As a result, the request blocked.

If a request to an electronic resource  $\in K_n$ , where n is from 1 to 17, the request will be allowed to the electronic resource, otherwise it will be blocked.

```

    select * from usertab where uid=' 'or a=a --' ...
    
```

### III. RESULT AND DISCUSSION

This section details the research results of the proposed security mechanism against data entry on the serve. Such attacks as SQL Injection must use a logical approach and reasonable input val-ues, together with the disruption of special characters of the source program accompanied by a normal SQL-query, to provoke the return of a tautologically correct value. If this type of attack applied to the authentication login page, the identity authentication mechanism can easily avoided and the login can successfully logged in. It means that the hacker has a legal right to access the system resource.

The most fundamental solution to defend against such attacks is to strengthen the verification mechanism of the application program. All input requires detailed checks to determine the purity of the input data values before passed to the downstream program for subsequent execution. In this way, we can eliminate the possibility of malicious input attacks. Regarding database access, experience shows that passing an SQL-query by string concatenation not only leads to security problems, as mentioned above, but also inadvertently leaks information about the database structure and the logical way the program works. A better approach is to send parameters to gain access to the database, together with checking the input parameters. This is more effective in preventing security problems. Control of responses to error messages need to strengthened. The user does not need to see much information. They can gather error messages from the database by trial and error, and then refine the attack.

The check must be strengthen for input values of a parameter if they contains special characters. For example, further processing is required for single quotes ('), semicolons (;) and left slashes (\) so that the combination of SQL syntax with these special characters can be treated as a word or sequence rather than part of language syntax

```

    select * from usertab where uid = '1989' ...
    
```

or grammar. Taking Citrix as an example, in its special character handling mechanism, if single quotes (") is encountered, an extra single quote is added before the character. Thus, the original characters will become purely symbolic because of this inverted comma. Combining the SQL-query in the process will not lead to unexpected results because of the logical judgement. For example, the original SQL looks like this:

If the malicious user input uid - with single quotes to replace 1989, such as 'or a = a--', the original sentence will become:

```
select * from usertab where uid=' 'or a=a --
```

The backend server will treat uid as an empty sequence and the grammar structure will return tautological TRUE; after contacting special characters acquire the following grammar:

Despite the fact that there is still a grammatical structure problem, at least it does not make the uid parameter values larger than a true logical constant. Similarly, whenever "\" (backslash) is encountered, we can simply insert an extra slash to the left before the character to take it out of subsequent characters; in case ";" (semicolon) is found, we can simply remove the characters to prevent the SQL syntax character from being erased, so it will not cut off the normal and unfinished statement following the semicolon

#### IV. CONCLUSION

This paper correlates the current prevailing methods according to their vulnerability to attacks and suggested protection attributes. We considered attacks based on string and command line operations and the corresponding protection mechanisms. If appropriate controls implemented correctly, it will effectively reduce the injection of SQL, cross-site scripting and other attacks. This results in a secure system environment. In conclusion, we can note the following results:

- The concept of adaptive protection of electronic resources from threats to information security, which allows to develop measures for the adaptive protection of resources using both signature and behavioural analysis, is proposed;

- An adaptive model of protection of electronic resources from threats to information security based on behavioral analysis was developed, this model allows to protect electronic resources from both those IS threats which already exist in the database, and new types of IS threats.

The developed adaptive mechanism will help to identify and make decisions on IS threats, with well-established and manageable means. Application of adaptive protection carries out control over popular IS threats and in time to provide protection and notification of the administrator, also such protection allows to apply a certain protection proceeding from type of IS threat. That is, adapt to the IS threat and apply the right protection.

#### REFERENCES

- [1] A. Makiou, Y. Begriche and A. Serhrouchni, "Improving Web Application Firewalls to detect advanced SQL injection attacks," presented at 10th International Conference on Information Assurance and Security, Japan, 2014.
- [2] E. Raff, J. Barker, J. Sylvester and R. Brandon, "Malware Detection by Eating a Whole EXE," presented at the Workshops of the Thirty-Second AAAI Conference on Artificial Intelligence, Ithaca, NY, 2017.
- [3] M. Ito and H. Iyatomi, "Web application firewall using character-level convolutional neural network," presented at the 14th International Colloquium on Signal Processing & Its Applications (CSPA), Penang, Malaysia, 2018.
- [4] K. Pranathi, S. Kranthi, A. Srisaila and P. Madhavilatha, "Attacks on Web Application Caused by Cross-Site Scripting," presented at the 2nd International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2018.
- [5] P. N. Joshi, N. Ravishankar, M. B. Raju and C. N. Ravi, "Encountering SQL Injection in Web Applications," presented at the 2nd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2018, pp. 257-261.
- [6] A. Jana, P. Bordoloi and D. Maity, "Input-based Analysis Approach to Prevent SQL Injection Attacks," presented at the 2020 IEEE Region 10 Symposium (TENSYMP), Dhaka, Bangladesh, 2020.
- [7] B. I. Mukhtar and M. A. Azer, "Evaluating the Modsecurity Web Application Firewall Against SQL Injection Attacks," presented at the 15th International Conference on Computer Engineering and Systems (ICES), Cairo, Egypt, 2020.

# Wireless security issues

**Kaloyan Kolev**

National Military University  
Veliko Tarnovo, Bulgaria  
kolevkaloqn35@gmail.com

**Yordan Shterev**

National Military University  
Veliko Tarnovo, Bulgaria  
jshterev@abv.bg

**Abstract.** Wireless home networks, for small organizations, as well as multi-user institutions and public networks need to be secured. This is a topical issue, especially since wireless protocols do not always provide good protection. The article aims to discuss the vulnerabilities and privacy security issues associated with wireless networks. The tools airmon-ng for monitoring, WireShark for snooping, aircrack-ng for dictionary pre-generation and also airodump-ng and aireplay-ng present in Kali Linux were used. The results of attacks and penetration tests performed on an experimental wireless connection protected with WPA2 show the vulnerability of wireless networks protected with this protocol. Therefore, accelerated implementation of WPA3 protocol is imperative.

**Keywords:** attacks, Kali Linux, security issues, wireless networks.

## I. INTRODUCTION

Introduction Wireless networks use radio waves to connect devices. These include notebook computers, desktop computers, personal digital assistants (PDAs), cellular phones, pagers, and more. Wireless networks work similarly to wired networks to transmit and receive information. They serve many purposes. In some cases, they are used as an alternative to wired networks, while in others they are used to provide access to corporate and personal data from remote locations. Wireless infrastructure is built at significantly lower costs than wired networks. They provide the local or business community with cheaper and easier access to information. Wireless networks allow remote devices to connect at a certain distance from each other. This makes the use of wireless technology very popular and rapidly spreading [1,2,3,4,5].

Wireless networks are rapidly expanding their capabilities. In addition to this, their bandwidth also increases. Due to their flexibility and freedom, they become an alternative communication infrastructure. Wireless communication provides users with the ability to exchange data at any time, with almost anyone, from anywhere in a communication channel. Because wireless communication and the Internet are compatible, users rely on communication to be secure and accessible. Data that is sent and received over the network is expected to be guaranteed to:

- authentication (sender and recipient are who they say they are);
- confidentiality (the message cannot be understood and read except by the recipient);
- integrity (the message has not been altered in integrity and content) [6].

For small organizations or in home networks, WLAN is a widely preferred solution. It can replace wired LAN and offers many advantages. Apart from them, the disadvantages should also be considered. As such, security can be cited compared to wired networks. It is an aspect that needs to be researched, especially in multi-user and public networks [7].

Improperly secured wireless networks can be used to infiltrate companies, banks, and government organizations. The frequency of these attacks increases due to ignorance and lack of analysis to secure wireless networks in a reliable manner [8,9].

Weaknesses and loopholes of Wi-Fi networks protected with protocols of the 802.11 standard – WPA2-PSK [7, 17, 20, 21] are researched with Kali Linux tools and computers with a wireless connection. The same protocols are widespread and the advanced WPA3 protocol is not yet widely used. Access to office, institutional and public wireless networks put the mobile devices in use at risk. Therefore, a similar study was carried out here, but using a computer with a wireless connection for analysis, and two mobile devices were used for users (clients of the network).

This article aims to discuss the vulnerabilities, weaknesses and privacy security issues associated with wireless networks. Separately, the results of attack and penetration tests performed on experimental wireless networks using the Kali Linux distribution are shown and analyzed.

## II. WI-FI NETWORKS SAFETY REVIEW

WLAN networks work according to the concept of the Open Systems Interconnection model (OSI model) [10]. Communication takes place through frames (packets), which are a sequence of bits. Each frame has a certain fixed length, which is determined by the type of transmission medium [11]. Each frame consists of a

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8186>

© 2024 Kaloyan Kolev, Yordan Shterev. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

header and body and additional data from higher layers of the OSI model. They contain control information related to the recipient. The frames contain a mechanism for checking the integrity of the content during delivery. The recipient checks the integrity of the packet and then sends an acknowledgment of receipt. The frame header structure is shown in Figure 1.

From the header structure, the fields Type, Subtype and Wep are important for security.

The *Type* field specifies three types of WLAN frames:

*Management* - enable the maintenance of communication, represent the presence of the AP, as well as connecting and disconnecting to it;

*Control* - allow and facilitate the exchange of data between stations with as little loss as possible;

*Data frames* – represent the majority of Wi-Fi communication, as payload. They are limited to 2312 bytes in size, so they can be split into fragments. They carry the actual information sent between clients.

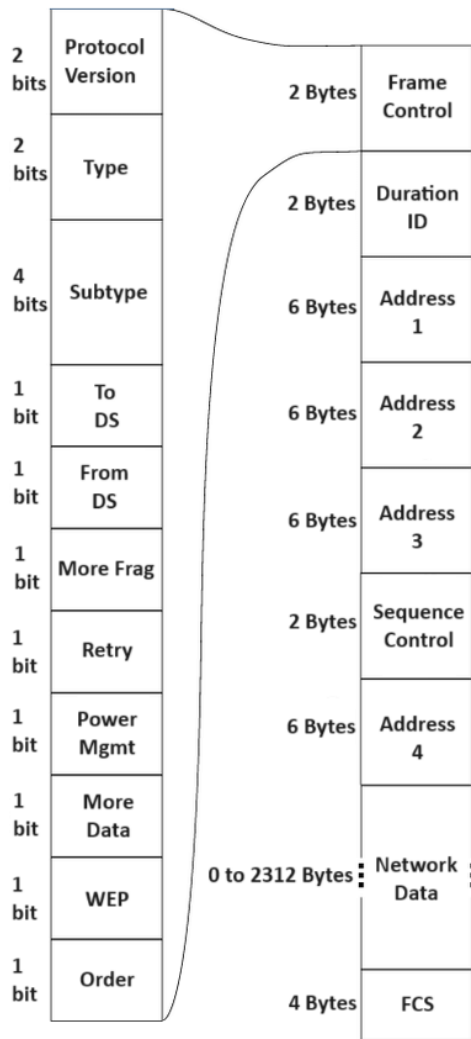


Fig. 1. Frame header structure

Control frames have the following subtypes from the *Subtype* field:

*Authentication* - sent by the client device as an authentication frame to the AP, contains information about its identity;

*Deauthentication* – sent by a wireless client that wants to terminate the connection to another client's network;

*Association Request* - sent by the client, allows the AP to synchronize and allocate resources. It carries information about the wireless connection, data rate and SSID if the AP is accepted, reserves memory and establishes an ID for the device;

*Response to the association request* – sent by the AP to the client and contains acceptance or rejection information;

*Reassociation Request* - a device sends a reassociation request when it goes out of range of the currently connected AP and finds another one with a stronger signal. The new AP coordinates the forwarding of any information that may still be contained in the previous AP's buffer;

*Reassociation Request Response* - sent by the AP, contains the acceptance or rejection of the device's reassociation request.

*Disassociation* – sent by a device that wants to disconnect. On receipt, the AP relinquishes the memory allocation and removes the device from the association table;

*Beacon* – sent periodically by the AP to announce its presence and provide the SSID and other pre-configured parameters;

*Probe request* – sent by a client when information is required from another client;

*Probe response* – sent by the AP, contains information about capabilities, such as supported data rates, etc. [12].

Control frames have the following subtypes:

- Request To Send (RTS);
- Clear To Send (CTS);
- Acknowledge (ACK) [8].

Encryption is one of the most important tools used to create a secure network.

Most APs offer the option of enabling one of the wireless encryption standards – Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2 or WPA3 [13].

WEP encrypts traffic using 64- and 128-bit keys. Encryption uses static keys, and every authorized system on the same network receives and exchanges encrypted messages using the same key.

WPA uses the Temporal Key Integrity Protocol (TKIP), which generates a new key for each individual packet. This type of encryption uses a 128-bit key and includes Rivest Cipher 4 (RC4) message integrity checks to determine whether there is interception and changes to data packets.

WPA2 uses the Advanced Encryption Standard (AES). It is more secure than RC4, the encryption standard used in TKIP and WEP. Cipher Block Chaining Message Authentication Code Protocol (CCMP) counter mode is also used to verify the integrity of encrypted packets. WPA2 operates in two modes, personal and enterprise. Private mode or Pre-Shared Key (PSK) relies on a shared key known to both the AP and the client device. Enterprise mode uses the more advanced Extensible Authentication Protocol (EAP) and uses an authentication server and individual credentials for each user or device on the wireless network.

WPA3 adds additional security to Personal and Enterprise modes. It uses individual data encryption. Each data transmission is encrypted with its own unique key. WPA3 uses a 192-bit key for personal mode and a 256-bit key for corporate mode.

In WPA3, AES is implemented using the Simultaneous Authentication of Equals (SAE) protocol, which provides better protection against offline attacks and password spoofing attempts by using stronger cryptographic algorithms and a more secure key exchange method [14].

A service set identifier (SSID) defines or extends a set of services. It is broadcast generally visible to all from an AP or other type of station in beacon packets. It announces and indicates the existence and presence of a network, which is visible to users as a name. The SSID can be customized with a length from zero to 256 bits [15].

Shared Key Authentication (SKA) is possible with the WEP encryption standard. It establishes in advance that the requesting system has knowledge of a shared key required for authentication. The key is delivered over the wireless network via a secure channel that is independent. The user only enters the password for a particular Wi-Fi network [16].

### III. MATERIALS and METHODS

A configuration consisting of a HP Pavilion 15.6-inch Laptop PC 15-eh1000 with Kali Linux operating system [17,18,19] equipped with a TP-link Archer T2U Plus AC600 wireless dual-band USB adapter. Samsung S20 mobile phone is used as the AP and Alpha 20 mobile phone is used as the client. The configuration of the AP is as follows: SSID: WirelessLab, Password: 12345679, Band: 2.4GHz, Security: WPA2-Personal, Broadcast channel: 1, MAC address type: Phone MAC and Hidden network: off.

The research was done in two stages with Kali Linux operating system. The first - checking for the hardware's ability to inject packets and the second - cracking a password on a Wi-Fi experimental network.

The research aims at the first stage to check with the specified hardware the possibility of packet injection.

In the second stage, possible password cracking in the Wi-Fi network is checked. For this purpose, a previously generated dictionary containing possible

passwords [8, 17] and the Kali Linux tools: Wireshark, airodump-ng, aireplay-ng and airmmon-ng was used.

### IV. RESULTS and DISCUSSION

For scanning and obtaining detailed information from the wireless interface in the form of a list of available APs in our range, the command: iwlist wlan0 s (scanning) is used in the terminal of the Linux distribution (fig. 2).

Wireless network cards have several modes of operation, according to their specific model. Most often, they are used as a managed mode subscriber station. Wireless network eavesdropping and packet injection requires the hardware to operate in monitor mode. In this configuration, it stops transmitting data and, on a pre-set channel, outputs the contents of all observed packets to the operating system.

```
(root@kali) ~/home/kaloyan
# iwlist wlan0 s
wlan0 Scan completed :
Cell 01 - Address: AE:6C:90:36:F0:75
ESSID:"WirelessLab"
Protocol:IEEE 802.11bgn
Mode:Master
Frequency:2.412 GHz (Channel 1)
Encryption key:on
Bit Rates:90 Mb/s
Extra:rsm_ie=30140100000fac040100000fac040100000fac020c00
IE: IEEE 802.11i/WPA2 Version 1
Group Cipher : CCMP
Pairwise Ciphers (1) : CCMP
Authentication Suites (1) : PSK
Quality=96/100 Signal level=-83/100
Extra:fm=000?
Cell 02 - Address: 5C:A4:F4:C3:30:CC
ESSID:"A1_30CC"
Protocol:IEEE 802.11bgn
Mode:Master
Frequency:2.427 GHz (Channel 4)
Encryption key:on
Bit Rates:130 Mb/s
Extra:wpa_ie=dd1a0050f20101000050f20202000050f2020050f20401000050f202
IE: WPA Version 1
Group Cipher : TKIP
Pairwise Ciphers (2) : TKIP CCMP
Authentication Suites (1) : PSK
```

Fig. 2 Command iwlist in Kali Linux.

To switch to monitor mode, use the airmmon-ng tool, which is available in the Kali Linux distribution (fig.3).

```
(root@kali) ~/home/kaloyan
# airmmon-ng start wlan0

PHY      Interface  Driver      Chipset
phy0     wlan0     88XXau     TP-Link Archer T2U PLUS [RTL8821AU]
          (monitor mode enabled)
```

Fig. 3 Starting monitor mode of Wi-Fi card with airmmon-ng.

Wireshark present in Kali Linux is used to eavesdrop on the wireless packets with the command wireshark [20] in the terminal. Select the used interface - wlan0 and filter packets only from the experimental network (fig. 4).

From the information given by the iwlist command, it is clear that the AP to which packets are injected works at a frequency from Channel 1 (2.412MHz)(fig. 2). For the effect to be possible, the antenna must be configured on the same channel as the AP. This is possible with the command: iwconfig wlan0 channel 1.

Restarting Wireshark and using a filter in the console to capture packets only from the experimental network: wlan.bssid == <MAC>, the name and MAC address of the AP are visible via iwlist.

A filter in the Wireshark console is used to perform an injection test:

```
wlan.fc.type_subtype == 0x08,
```

it outputs only non-beacon packets for the experimental network.



The next step is to inject using the *aireplay-ng* tool and the following command in a terminal:

```
aireplay-ng -9 -e WirelessLab -a <MAC> wlan0.
```

Wireshark observes multiple packets that are sent by *aireplay-ng*, and the output in terminal is: Injection is working! (fig. 5).

WPA2 PSK works by generating a session key between the AP and the client called a Pairwise Transient Key (PTK). It contains PMK, ANONCE, SNonce, MAC(AA) and MAC(SA). PSK is used to encrypt all data in the session between the AP and a specific client.

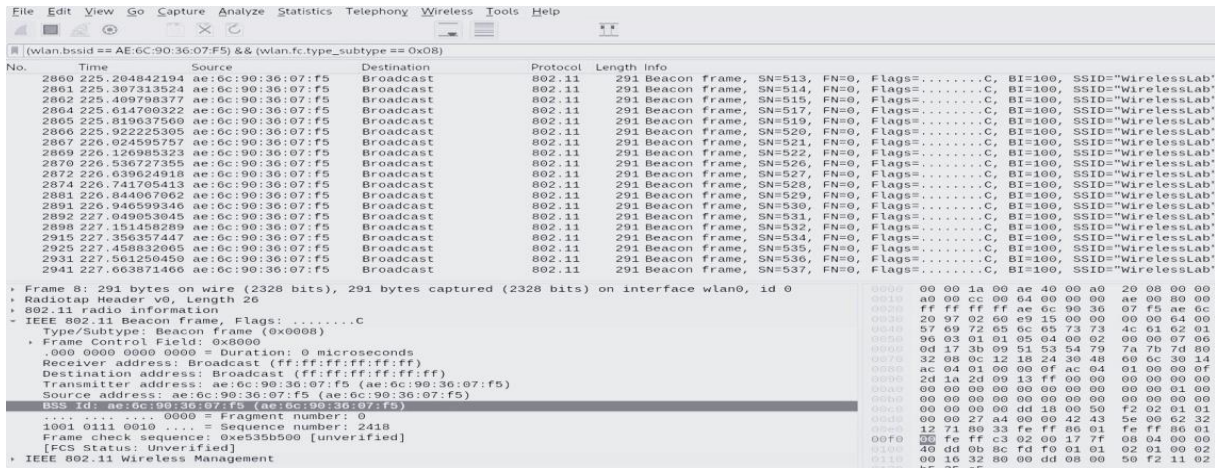


Fig. 4 View in Wireshark Screen in Kali Linux.



Fig. 5 Injection of packets in experimental Wi-Fi network.

Packet injection is a possibility for many attacks, such as denial of service (DoS), Man-in-the-middle attack (MIMT), as well as sending deauthentication packets, which is necessary when cracking passwords on Wi-Fi networks.

In the second stage, the vulnerability associated with the Pre-Shared Key (PSK) authentication scheme is used to crack the password of the experimental network. It is protected with WPA2 personal.

The password being searched for is PMK- Pairwise Master Key. PSK is a translated 256 bit string from PMK.

WPA2 PSK is created through a four-step data exchange process. In the first step, the AP sends to the client an Authenticator Nonce (ANonce), a random number generated by it. In the second stage, the client returns a Supplicant Nonce (SNonce) along with a Message Integrity Check (MIC). SNonce is a random number generated by the client and MIC is a message integrity code. In the third step, the AP sends the Group Temporal Key (GTK) to the client. It is the same for all network subscribers. In the fourth stage, the client sends data to the AP. They indicate that the key is installed and communication between them continues.

With WireShark in monitor mode, all communication between APs and clients can be viewed [20]. Only the PSK is not known when attempting to crack a password. It is retrieved as a combination provided by the user along with the SSID. It is sent via Password-Based Key Derivation (PBKDF2), which derives the 256-bit shared key.

A pre-generated dictionary of possible passwords is used to crack the password. The attack tool extracts the PSK and uses it in combination with the other parameters in it to create the PTK. It is used to check the MIC in one of the intercepted packets. If the combination of the tested password together with the other data matches, then the assumed password is correct.

The command tool is used to crack the experimental network password:

```
airodump-ng -bssid <MAC> --channel 1  
write WPAcrackDemo1234 wlan0. (fig. 6)
```



Fig. 6 View of terminal with use of airodump-ng

*Airodump-ng* displays information about the presence of the four-way *handshake* process and the MAC address of the client that performed it.

Injection sends deauthentication packets to all clients via:

```
aireplay-ng -0 5 0 -a <AP's MAC>.
```

Clients automatically or manually connect to the network. This process generates data.

The data from the four-way handshake process is stored in a file: WPACrackDemo1234.cap. It is used together with a pre-generated dictionary via the aircrack-ng tool with the command [21]:

```
aircrack-ng WPACrackDemo1234.cap -w  
/usr/share/wordlists/passwords.lst
```

Various combinations are tried by the method described above. If the password is present in the dictionary, the tool succeeds in cracking it on the experimental network. (fig. 7)



```
Aircrack-ng 1.7  
[00:23:04] 12304762/111111110 keys tested (9041.84 k/s)  
Time left: 3 hours, 2 minutes, 7 seconds 11.07%  
KEY FOUND! [ 12345679 ]  
  
Master Key : 93 B6 7D AF AC 84 0C 54 C1 F9 64 FD D9 7A 0D 6A  
            A7 9B BE B5 9A 86 33 18 33 D2 2B 04 08 68 BA 6B  
  
Transient Key : FD 62 8B 44 AE 57 2D CD 11 F7 40 AD 3E B3 5F 7E  
              8B D1 1A 0B B9 94 F4 0A E0 5C D6 00 00 00 00 00  
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
  
EAPOL HMAC : E2 46 E0 E5 58 76 A3 DE 01 16 CA C8 4F A7 99 82
```

Fig. 7 Result of cracking password with aircrack-ng

### CONCLUSIONS

The article reviews key aspects of the information security of Wi-Fi networks - protocols, keys, security fields in the data packet headers. Separately, research has been carried out under Kali Linux operating system for packet injection and password cracking in a Wi-Fi experimental network. The tools airmon-ng for monitoring, Wireshark for snooping, aircrack-ng for dictionary pre-generation and also airodump-ng and aireplay-ng present in Kali Linux were used.

The research results show that packet injection and password cracking are possible using the Kali Linux tools used and a pre-generated dictionary. This confirms the weaknesses and gaps in the security of Wi-Fi networks protected with the WPA2-PSK protocols for mobile client devices. It also indicates the need to accelerate the transition to the WPA3 protocol.

Investigations with other tools including the Kali Linux operating system for Wi-Fi vulnerabilities is a future field of research.

### 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] Salazar J., Wireless networks., Czech Technical University of Prague.
- [2] Mehdi Khosrow, Steve Clarke, Murray E. Jennex, Annie Becker, Ari-Veikko Anttiroiko, Wireless Technologies: Concepts, Methodologies, Tools and Applications, Volume I, Published in the United States of America by Information Science Reference, ISBN 978-1-61350-102-3 (ebook), 2012 by IGI Globa.
- [3] Fundamentals of wireless sensor networks Walteneus Dargie, Christian Poellabauer, ISBN 978-0-470-99765-9, Published by John Wiley & Sons Ltd, 2010.
- [4] Ivan Stojmenovic, Handbook of wireless networks and mobile computing, ISBN 0-471-22456-12002, Published by John Wiley & Sons, 2002.
- [5] Matthew Gast, 802.11 Wireless Networks The Definitive Guide, Publisher: O'Reilly, ISBN: 0-596-10052-3, April 2005.
- [6] Boncella R.J., Wireless Security: An Overview., Washburn University.
- [7] Jaiaree T., The security aspects of wireless localarea network (WLAN)., Monterey, California Thesis.
- [8] Buchanan C., Ramachandran V., Kali Linux Wireless Penetration Testing Beginner's Guide - Third Edition, Packt Publishing.
- [9] Gregory Kipper, Wireless crime and forensic investigation, , Auerbach Publications Taylor & Francis Group, ISBN-10: 0-8493-3188-9, 2007.
- [10] ISO/IEC 7498-1:1994, Information technology Open Systems Interconnection Basic Reference Model: The Basic Model.
- [11] Георгиев. В., Вградени и автономни системи. София, Университетско издателство „Св. Климент Охридски“, 2014.
- [12] <https://www.ii.pwr.edu.pl/~kano/course/module8/8.2.1.4/8.2.1.4.html> [Accessed: January, 2024].
- [13] <https://www.techtarget.com/searchnetworking/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2> [Accessed: January, 2024].
- [14] <https://www.nordvpn.com/blog/wep-vs-wpa-vs-wpa2-vs-wpa3/> [Accessed: January, 2024].
- [15] Terry L.; Barber, Simon, eds. (2007), "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (IEEE Std 802.11-2007).
- [16] Rouse M., "Shared Key Authentication", Technopedia.
- [17] <https://www.kali.org/> [Accessed: January, 2024].
- [18] Ric Messie, Learning Kali Linux, ISBN: 9781492028697, O'Reilly Media, 2018 July.
- [19] Sanjib Sinha, Beginning Ethical Hacking with Kali Linux, ISBN-13 (electronic): 978-1-4842-3891-2, 2018.
- [20] <https://www.wireshark.org/> [Accessed: January, 2024].
- [21] <https://www.aircrack-ng.org/> [Accessed: January, 2024].

# *The contribution of the Military school to the building of the national security system of Bulgaria in the period 1878-1885*

**Krastyu Ivanov Krastev**

Specialized Training Department, Security and Defence Faculty,  
Vasil Levski national Military University,  
Veliko Tarnovo, Bulgaria  
kikrastev@nvu.bg

**Abstract.** The present article is part of an in-depth scientific study focused on the evolution of officer training in the Bulgarian military school from 1878 to the present day. The subject of this report is the role of the military school in the developing system of national security in the period 1878-1885. The purpose of the report is to determine the contribution of the military school to national security based on the analysis of quantitative and qualitative indicators. To achieve the goal, the following research tasks have been formulated: 1. To carry out a study of the available military-historical archival funds and units to establish the parameters of the quantitative and qualitative indicators of the study. 2. Based on the analysis of the career development of officers who successfully graduated from the military school, to determine their contribution to national security for the period of study. The research methodology covers the use alone or in combination of the generally accepted scientific methods of analysis and synthesis, comparison, induction and deduction, historical references, studies of specialized publications on the subject, etc.

**Keywords:** military school, Bulgaria, national security

## I. INTRODUCTION

The role of the military education system in the national security system is the subject of research by many modern Bulgarian scientists. Some of them research the modern approaches to education and management in the system of security (Stoykov S., Marinov P., 2019) [1], the influence of military organizational culture on individual performance of the learners (Petrova E., 2019) [2], the styles of management for military security systems (Marinov R., 2020) [3], as well the leadership style of the Bulgarian cadets as a part of national security education process (Atanasova-Krasteva, 2015) [4].

And while the role of the military school in its modern form is the object of constant research by military specialists, it is striking that there is insufficient research on the initial stage of the process of creation and development of the military school, as the basis of statehood and the

security system in Bulgaria, namely the period 1878-1885. After the end of the Russian-Turkish War, Bulgaria gained its independence after a long period of Ottoman rule. According to Article 6 of the preliminary San Stefano peace treaty, a Russian occupation army remains on the territory of liberated Bulgaria for a period of 2 years to maintain order and protect the state and to provide its national security. Later according to Art. 22 of the Berlin Treaty, this period is reduced to 9 months. [5]

Prince Dondukov-Korsakov, who was appointed on 08.05.1878 as the Imperial Russian Commissar in Bulgaria, understood very well that after its liberation, Bulgaria would need a strong army to defend its conquests. For this new established army, command staff will be needed, which it cannot get anywhere, but must train and prepare itself. Moreover, the acceptance of the first set of 30,000 young men into the Land Army is scheduled for the month of September 1878. That is why one of the first steps of the Imperial Russian Commissar was to establish as soon as possible an institution for the training of junior officers. While the issue of non-commissioned officers can be resolved with the recruitment of personnel from the militia companies, the issue of officers remains open. Indeed, in the Russian army there is a core of 36 Bulgarian officers, mostly junior officers, but a small part of them are in the Balkan theatre of military operations.

The present article is part of an in-depth scientific study dedicated to the development of officer training in the Bulgarian military school from 1878 to the present day.

## II. MATERIALS AND METHODS

According to the research results of the available electronic database in Bulgarian State Military Archive Agency, the archival fund of the Bulgarian military school consists of 39 inventories with a total of 2,774 archival papers and documents covering the period 1878 - 2001. They are the main open sources of historical information for the fundamental research of which this article is a part.

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8231>

© 2024 Krastyu Ivanov Krastev. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

The subject of this report is the role of the military school in the national security system developing process in the period 1878-1885.

The purpose of the article is to research and determine the contribution of the military school to national security based on the analysis of quantitative and qualitative indicators.

To achieve the main research goals, the following research tasks have been formulated:

1. To research the available military-historical archival funds and units to establish the parameters of the quantitative and qualitative indicators of the study.

2. Based on the analysis of the career development of officers who successfully graduated from the military school, to determine their contribution to national security for the period of study.

The research methodology covers the use alone or in combination of the generally accepted scientific methods of analysis and synthesis, comparison, induction and deduction, historical references, studies of specialized scientific publications on the subject, etc.

### III. RESULTS AND DISCUSSION

1. Establishment of a military school - the strategic move of the Imperial Commissar.

According to a number of specialists who have worked on the subject (Zlatev M., 2004; Ruchev N., 2012) [6], [7], the establishment of the military school at the dawn of the newly liberated state is of extreme importance for statehood in Bulgaria. Even before the decisions of the Berlin Congress regarding the future fate of the newly established Bulgarian principality, according to the Treaty of San Stefano were known, the Imperial Commissioner in Bulgaria, Prince Dondukov-Korsakov, fearing an unfavorable decision by the Congress on the period for the stay of Russian troops on the territory of The Principality proceeded to form in Plovdiv a military training unit, composed of Bulgarian youths, who were to be given elementary military training, so that, if political circumstances required, they could be produced in the first rank of officers and fill the command staff of the newly created Bulgarian Land army. This strategic move aims to prevent the recruitment and entry into the army of foreign officers.

The main specialist in Bulgarian military history (Zlatev M., 2004) [8] define the beginning of this first period in the creation of the military school in Bulgaria as a period of searching for the optimal option in the construction of the military school in a country that has just gained freedom after 500 years of slavery, which lacks a suitable personnel potential to create officer corps. The choice of the best option is influenced by an extraordinary number of circumstances that are difficult to summarize and accept.

The analysis of the socio-political situation in national and international aspects reveals several main factors that have a negative character in relation to the idea of creating a military school. In the first place is the training time, or rather the lack of sufficient time for the training of an

officer, according to the political circumstances of the period.

The other main challenges at the beginning are:

- the absence of own personnel and teaching staff to conduct the officer military training,

- lack of theoretical and applied materials for military training and training of officers - instructions, doctrines, field manuals, etc.,

- there is no educational and material base for military training,

- weak or almost non-existent general educational training of incoming cadet candidates,

- language barrier in the use of Russian teachers and instructors,

- complete absence of historical experience and traditions in military officer training, etc.

Therefore, we should not be surprised at the frequent changes, numerous compromises and not always adequate solutions in the process of these searches.

It is enough to mention even just the wandering in determining the period of training from several months to five years, and in later periods and 6-7 years, in order to assess the difficulties faced by the first builders of the Bulgarian military school.

2. The command of the "volunteers".

On March 1878, a Russian language course was opened in Plovdiv with the task of preparing young people for translators and secretaries in the newly appointed district administrations and other state departments in the new established Bulgaria. The course participants are 120 people from all over the country, mostly graduates of the best grade schools, as well as high schools abroad. Classes are held at Holy Trinity School. The course is led by the Russian captain Nikolai Fedyai, and the director is Grigor Nachovich. The director Nachovich informed all students that very soon a military school for the training of officers would be opened in Sofia. Before that, he informed them that a military training command was being opened in Plovdiv. The so-called command of the "volunteers" in which they will be able to enter and which will become the germ of the future military school. At the end of May 1878, in the lower floor of the former Turkish inn in Plovdiv, guard captain Nikolay Fleischer accepted requests to join the command, where 40 people enrolled in the translator course. Captain Fleischer takes over the senior control and organization of the classes. In August 1878, this command already numbered 80 people and was renamed a company of volunteers. Many of those who enrolled graduated from Aprilov High School, Plovdiv Grade School, Bolgrad Bulgarian High School, Robert College and Galatasaray Lyceum in Constantinople and other educational institutions abroad. At the same time, Prince Dondukov-Korsakov instructed the head of the military department of the Imperial Commissariat, Major General Zolotarev, to study the issue of establishing a military school in the country as soon as possible and to do everything possible for its soon opening. From the very beginning of the formation of this command, intense classes began to be

held with it. This is necessary in view of the possible danger that the graduates will be produced earlier in the first officer rank. In addition to conducting drills, lectures on topography were given by staff captain Ryabinkin and on fortification by engineer captain Saranchov. When, after the signing of the Treaty of Berlin on 01/07/1878, it became known that the Russian occupation troops would remain in the Principality of Bulgaria and Eastern Rumelia for 9 months, not 2 years, and when around the middle of August 1878 the first reports appeared about the establishment of a military school, training in the command is limited almost exclusively to military training with the desire for the upcoming major military ceremony to present itself in the best possible way. After the ceremony, the company's classes are almost suspended, because preparations are already being made for its departure to Sofia to enter the military school. In the first days of August 1878 Major General Zolotarev drew up a proposal and after its approval, on 15-08, a notice was published for the knowledge of the Bulgarian youth for admission to the newly established military school. In the initial situation for the establishment of the military school, some main principles were laid down, which were in force for a long period of its existence. The aims of the school are stated very briefly, but still clearly enough. Only one military school is established for all branches of troops, which is of fundamental importance for the uniformity of the officer corps. Unfortunately, in later periods these principles were drastically violated in favour of the recognition of the role of the Bulgarian officers. Recently after the announcement, the program for the entrance exam of the candidates was also announced. Of interest are not only the subjects on which they will be tested, but the main questions on which they must demonstrate knowledge. The program was published in issue 16 on 19-th of September 1878 of Maritsa newspaper. The program for the entrance exam for admission to the junior class includes the disciplines of God's law, Russian language, Bulgarian language, mathematics, arithmetic, geography and history. The examination program for the senior class includes the disciplines of God's law, Russian language, Bulgarian language, mathematics, arithmetic, geometry, geography and history. The newly established military school was under the department of the Imperial Commissar and under the authority of the member of the council and the head of the military department. The Imperial Commissar has the highest supervision in the direction of the educational part. The closest management of the school is assigned to its head. The military school has a study committee and a library.

### 3. Terms of study.

When establishing a school, cadets are accepted simultaneously for 2 classes for a training period of 1 year for the senior class and 2 years for the junior class. However, due to the complicated situation in Bulgaria after the decisions of the Berlin Congress, the training of the first graduating class was shortened and they were produced as officers on 10/05/1879, that is, after staying at the school for about 5 and a half months. In 1880 it was concluded that a two-year course of study was insufficient to thoroughly pass the material, both in educational and military subjects. Therefore, by order of the military department No. 156 of the same year, it was ordered to switch to a 3-year training

period from the academic year 1881-1882. Subsequently, it was judged that this was insufficient and real since 1881. year the school is on a four-year course, having the following classes – junior class, senior class, main first special class and second special class. At the beginning of the next academic year, the fall of 1882 one more main class is opened, called preparatory class, which makes the full course of the school 5 years. However, this continued until the autumn of 1884, when the duration was again switched to 4 years of training, which was considered to be quite sufficient to give the necessary theoretical and practical training to future officers. After the Serbo-Bulgarian war of 1885, due to the premature production of the cadets of the senior class and their sending to the front, the number of trainees in the school decreased and again it was switched to a 3-year training course.

In 1888, another preparatory class was opened, which made the training period four years again. This situation in the school was preserved until the end of the century.

In 1900, serious changes took place in the school. They are mostly related to the opening of a military high school for him. The credit for this goes to the then chief, Colonel Mikhail Savov, and the class inspector, Captain Nerezov. The reason for the change is primarily the aspiration of the school's command to reach the European level in the training of officer cadres. By starting their education and upbringing at an early age. Undoubtedly, this is one of the ways to achieve better military training of the future young officers. [9]

### 4. Analysis of the realization of the graduates of the military school for the period 1879-1900.

In order to properly analyse the realization of the graduates of the military school for the period 1879-1900, it is necessary to correctly select the indicators through which we can obtain the necessary results.

For the purposes of the present study, we can use as quantities indicators Tcad (total number of accepted cadets) and SGrad (number of successful graduates) as quantitative indicators. As an indicator of the effectiveness of the training received in the military school is the realization of the graduates in the professional career, denoted by Rprof (professional realization).

TABLE 1 RESEARCH INDICATORS

Graduated classes	Research indicators		
	Tcad	SGrad	Rprof
1 graduated class	252	163	36
2 graduated class	177	84	14
3 graduated class	139	62	7
4 graduated class	72	50	13
5 graduated class	95	45	7
6 graduated class	93	58	17
7 graduated class	112	74	3

Source: created by author

First graduated class – 10/05/1879

The value of Tcad<sub>1</sub>= 252 represent the total number of accepted cadet candidates in the first graduated class. The

value of the indicator  $SGrad_1 = 163$  shows to us that 64,68% from the cadets successfully graduated the military school.

As a quality indicator  $Rprof_1 = 36$  (22,09%) is representing the number of the successfully graduated who achieved the highest possible duty rank – General. The first group is so called “General graduation group”, due to the largest number (36) of graduated who later in the military carrier became Generals. It is interesting to note that till 1913, 83 (50,92%) of them commanded regiments, 42 (25,77%) brigades, 15 (9,20%) divisions, and 8 (4,90%) armies. In addition, 5 became heads of the military school, 3 became inspectors of artillery 2 of cavalry, 5 officers reach the rank of chief of the army staff, 6 officers reach the top of the career and become ministers of defence.

#### Second graduated class – 30/08/1980

As shown on the Tab. 1 the value of  $Tcad_2 = 177$  means that the second cadets group is about 70,24% from  $Tcad_1 = 252$  as total amount of the cadets accepted one year earlier. The value of indicator  $SGrad_2 = 84$  shows that only 47,46% of all accepted cadets successfully graduated military school. After a two-year training course graduated 84 infantry officers, 62 artillerymen, 11 cavalrymen, 7 and 4 engineer officers.  $Rprof_2 = 4$  is the quality indicator and it represents the realization of 16,67% of successfully graduated who achieved the highest rank in military carrier.

#### Third graduated class – 30/08/1882

$Tcad_3 = 139$  candidates entered (21,47% less than the previous year), and  $SGrad_3 = 62$  (44,60%) cadets successfully graduated, of which  $Rprof_3 = 7$  (11,29%) reached the rank of general.

#### Fourth graduated class – 30/08/1883

In the 4th graduating class,  $Tcad_4 = 72$  (48,20% less than the previous year) candidates entered, who study for 4 years. They graduated earlier that it had been scheduled on 30/08/1883, with  $SGrad_4 = 50$  (69,44%). From them,  $Rprof_4 = 13$  (26%) officers reached the rank of general.

#### Fifth graduated class – 30/08/1884

The fifth graduating class of  $Tcad_5 = 95$  (31,94% more than the previous year) candidates was admitted to the school on 09/19/1880. The graduation was on 30/08/1884, when  $SGrad_5 = 45$  (47,37%) people became officers. Of these,  $Rprof_5 = 7$  (15,56%) officers reached the rank of general.

#### Sixth graduated class – 30/08/1885

In May 1881 a total of  $Tcad_6 = 93$  candidates were admitted to the school in the 6th graduating group. Graduation took place on 30/08/1885.  $SGrad_6 = 58$  (62,37%) became officers. Of these,  $Rprof_6 = 17$  (29,31%) officers reached the rank of general.

#### Seventh graduated class – graduated in the combat units

The seventh graduating class entered in 1882 for a four-year study period. The values of indicators are  $Tcad_7 = 112$  (20,43% more),  $SGrad_7 = 74$  (66,07%). The Serbian-Bulgarian war, which began in 1885, required that the graduating class be produced ahead of schedule in the rank of portupty-junker and sent to the front line. Later, without

returning to the school, at different times they were promoted to officer ranks. From this graduating class,  $Rprof_7 = 3$  (4,05%) officers reached the rank of general.

## IV. CONCLUSIONS

1. Already at the dawn of post-liberation Bulgaria, we can define the idea of guaranteeing the security of the nation by establishing of a military school for the training of officers for the needs of the Bulgarian Land Forces as a strategic decision in the field of national security.

2. Despite the difficulties and the absence of minimum necessary conditions for training - qualified teachers, necessary study materials, study-material base, national traditions and experience in the training of officers, etc. the leadership of the military school, by applying "ad hoc" solutions, managed to prepare the necessary officer cadres for the young Bulgarian army.

3. Despite the insufficient time and conditions for the research period of 1878 until 1885 the military school managed to prepare 536 officers who with their expertise build the national security system in its military component, with 87 of the graduates reaching in their carrier the rank of general. The analysis highlights the achievements of the first graduating class, called "general class", from which by 1913, 83 of them commanded regiments, 42 commanded brigades, 15 commanded divisions, and 8 commanded armies. In addition, 5 became heads of the military school, 3 became inspectors of artillery 2 became inspectors of cavalry, 5 officers reach the rank of chief of the army staff, 6 officers reach the top of their careers and became ministers.

4. The analysis of the origin and development of the military school in the studied period reveals that it was established with Russian support in 1878 in the city of Plovdiv, subsequently moved to the city of Sofia, where it was officially opened, which gives us reason to assume that with its establishment, the beginning of the construction of the military-educational system, as an fundamental element of the national security system of Bulgaria in the end of the XIX century.

## REFERENCES

- [1] Stoykov S., Marinov P. (2019). A comprehensive approach to education and management in the system of security, National Defense University “Carol I”, The 15th International Scientific Conference “Strategies XXI”, Volume XV, Part 1, ISSN 2668-201X, ISSN- L 2668-201X, p.p. 348-353
- [2] Petrova E. (2019). Influence of Military Organizational Culture on Individual Performance of The Learners of the Example of The Vasil Levski National Military University, Bulgaria, International Conference on Creative Business for Smart and Sustainable Growth (CREBUS), 2019, pp. 1-4, Electronic ISBN:978-1-7281-3467-3. CD:978-1-7281-3466-6. Print on Demand(PoD) ISBN:978-1-7281-3468-0
- [3] Marinov R. (2020). Styles of Management for Military Security Systems, KSI Transactions on, Knowledge Society A publication of the Knowledge Society Institute, Volume XIII, Number 2, p.p.24-27, June 2020, ISSN 1313-4787, <http://www.tksi.org/Archives.htm>, EBSCO
- [4] Atanasova-Krasteva N. (2015). Comparative analysis of the leadership style of the bulgarian cadets – part in the national security education, The 24th international scientific conference Knowledge-Based Organization, Economic, social and administrative approaches to the knowledge-based organization, vol. XXIV, No 2, p. 255-260, Sibiu, Romania, 2015, ISSN 1843-682X

- [5] Holland, Thomas Erskine (1885), "The Preliminary Treaty of Peace, signed at San Stefano, 17 March 1878", *The European Concert in the Eastern Question and Other Public Acts*, Oxford: Clarendon Press, pp. 335–348, retrieved 2024-03-14
- [6] Ruhchev N., *The Military School of Bulgaria 1878 – 2002*, MoD Publ., Sofia, 2012 ISBN 978-954-9971-644, pp.17-73
- [7] Zlatev M., *The Military School on the Eve of the Serbian-Bulgarian War 1885*. In: *The Military Defense of the Union*, pp. 47-52, Sofia, 2006.
- [8] Zlatev M., *The military school - the backbone of the Bulgarian military education system*, *Vezni mag.*, special issue, Sofia, 2004, pp. 11-17.  
Zlatev M., *125 years of Bulgarian military education*, *Scientific works of Vasil Levski National University*, Vol. 73-I, 2003, pp. 12-19.

# A Preliminary Study of Photon Radiation Attenuation from Ballistic Protection Materials

**Krasimir Kalev**  
Faculty APVO&CIS  
NMU Vasil Levski  
Shumen, Bulgaria  
kraskalev@abv.bg

**Lyubomir Manov**  
Faculty APVO&CIS  
NMU Vasil Levski  
Shumen, Bulgaria  
3lemlem@gmail.com

**Abstract.** Modern ballistic protection equipment is lightweight, flexible, and withstand multiple types of threats. Depending on their purpose, they are assembled from various materials, with ceramic plates and composites based on high-performance polymer fibers finding wide application in recent years. Multilayer fabrics with different textures woven from synthesized special mechanically high-resistant polymer fibers successfully withstand the high-speed and high-energy impact of the striking element. Given the risk of exposure to radiation during military conflicts or industrial accidents, it is necessary to know the anti-radiation parameters of protection means. The report attempts to establish the degree of protection against photon radiation in the range of 40 KeV to 120 KeV for samples of ballistic panels with ballistic protection levels III+, III++, and IV. The degree of attenuation of photon radiation with these energies was measured by irradiating the examined ballistic panels. A dose-dependence has been obtained with level of ballistic protection for the specific material as a function of the energy of photon irradiation.

**Keywords:** radiation safety, attenuation coefficient, hard armor plate.

## I. INTRODUCTION

In the modern conditions of the evolution of human society in the development of military conflicts and industrial accidents (accidental or intentional) in infrastructure facilities using intensive production technologies with unconventional energy sources, there is a critical factor of occurrence of radiation that is more powerful than the allowable natural radiation pool. Part of this radiation is ionizing radiation, which passes through matter and ionizes it, adversely affecting human life.

Technological advances in obtaining new more efficient materials used in ballistic protection such as ultra-high molecular weight polyethylene (UHMWPE), carbon nanotubes, liquid armor, graphene, composites,

etc. are also leading to better photon radiation protection capabilities!?

On the other hand, there are experimental trials of standard means of individual ballistic protection through which the possibility of radiological examination of a patient wearing protective body armor has been established [1]. In cases of combat injury, this reduces the time required for preliminary diagnosis, as the ballistic protective equipment need not be removed and the appropriate medical procedure can be carried out on time.

Polymer composites are generally not suitable for attenuation of photon radiation due to the low content of high-order elements from the Mendeleev table. In recent years, attempts have been made to incorporate classical high atomic number elements (PbO) into polymer matrices, thereby increasing the shielding capability. Moreover, there are studies in which the protective lead oxide has been replaced by low-toxicity lead-free shielding compounds [2].

Regardless of the degree of exposure, it is unacceptable to underestimate the invisible and insensitive effects of photon radiation on human organs. Therefore, it is necessary to know to what extent the generally accepted (traditional) clothing and means of individual ballistic protection of servicemen, depending on the structural composition and geometrical parameters protect and absorb radiation. The purpose of this paper is to present experimental data on the degree of radiation attenuation in irradiation of a certain type of hard body armor with ballistic protection levels according to a generally accepted NATO standard [6].

## II. MATERIALS AND METHODS

### 2.1. Hard Body Armor

Currently, the most widely used materials in the manufacture of ballistic protection devices in the hard

Print ISSN 1691-5402  
Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8221>

© 2024 Krasimir Kalev, Lyubomir Manov. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)



armor segment are based on polymers and ceramics, and in the combat helmets segment on polymers of the aramid and kevlar type [3], [4].

Hard Body Armor MARS Armor® was used for the study [11]. They are designed to protect the human body mainly from bullets and fragments and consist of Ballistic Inserts and Plate Carriers.

The Ballistic Inserts represent Plates to protect from high-velocity ammunition, including rifle and machine gun fire (also by using a silencer [5]). Plate Carriers are designed to provide maximum coverage and protection, with good mobility and wearing comfort of the Ballistic Inserts types.

Six types of Ballistic Inserts with different levels of protection were investigated in the active laboratory experiment. The general device of Ballistic Inserts or Ballistic Panel consists of a Plate and a Substrate (Backing). A hybrid type of Ballistic Insert it is composed of two parts ceramic and high molecular weight polyethylene.

1) Ballistic Insert, hybrid type, Protection level III+, Standart NIJ 0101.04.

The Plate has a composition of ceramic SiC with dimensions - 250x300 mm and thickness – 6 mm.

The Substrate has a composition of compressed high molecular weight polyethylene Dyneema HB50 with thickness – 11 mm.

2) Ballistic Insert, hybrid type, Protection level III++, Standart NIJ 0101.04.

The Plate has a composition of ceramic SiC with dimensions - 250x300 mm and thickness – 6 mm.

The Substrate has a composition of compressed high molecular weight polyethylene Dyneema HB80 with thickness – 11 mm.

3) Ballistic Insert, hybrid type, Protection level IV, Standart NIJ 0101.04.

The Plate has a composition of ceramic SiC with dimensions - 250x300 mm and thickness – 10 mm.

The Substrate has a composition of compressed high molecular weight polyethylene Dyneema HB80 with thickness – 10 mm.

4) Ballistic plate made of ceramic Al<sub>2</sub>O<sub>3</sub> with dimensions - 245x285 mm and thickness – 10 mm.

5) Substrate made of compressed high molecular weight polyethylene FMS H62 with thickness – 15.6 mm.

6) Successfully tested Ballistic Insert in a seven-shot firing with an 7.62x39mm AP cartridge. Ballistic Insert is a hybrid type, Protection level III+, Standart NIJ 0101.04. The Plate has a composition of ceramic SiC with dimensions - 250x300 mm and thickness – 6 mm. The Substrate has a composition of compressed high molecular weight polyethylene Dyneema HB80 with thickness – 11 mm.



Fig.1 Ballistic Inserts with different levels of protection.

## 2.2. Experiment setup

For the experiment, PHILIPS Diagnost 1 and Siemens Polymat 70 diagnostic X-ray units were used. Both X-ray units allow obtaining and precisely controlling the X-ray radiation parameters in the desired range as well as adjusting the geometrical parameters of the experiment. The X-ray units have the necessary certificates for normal operation.

To measure the actual values of the quantities characterizing the X-ray radiation, a solid state detector-dosimeter Radcal AGMS-DM+, Solid State kV/Dose Multisensor using Accu-Gold+ Digitizer and Accu-Gold Software was used [9]. The Accu-Gold+ system used allows for measurement of the maximum energy of the generated X-ray pulse in the form of maximum pulse kilovolts, average kilovolts, absorbed dose, dose rate, pulse duration, half attenuation layer, pulse shape as well as total filtration.

The Accu-Gold+ system used has undergone calibration and certification with a certificate issued on 08.2023 by MEDEIX LAB SofiMae France [10].

The geometrical configuration of the experiment is as follows: the Ballistic Plate is placed on top of a horizontally positioned table with the center coinciding with the center of the X-ray beam. The distance between the work table and the focal point of the radiation generator is set to 1 m. The field of the generated beam is selected to completely cover the object. The beam is generated vertically downwards. The detector is placed along the beam axis once on or below the plate. The measurements on and under the plate are taken with the same set of X-ray parameters [7].

## III. RESULTS AND DISCUSSION

During the measurements, the radiation intensity was kept constant by keeping the generator current and pulse duration constant at 100 mA and 100 ms. The pulse energy is controlled by setting the accelerating voltage in the X-ray generator. A higher accelerating voltage at the same current and time gives a higher pulse energy.

After the X-ray pulse is generated and until it reaches the point of measurement, the pulse undergoes attenuation due to absorption partially in the exit window of the X-ray tube and other structural materials in the beam path. This type of absorption and scattering is called self-filtration of the X-ray generator. Filtration modifies the energy spectrum of the outgoing radiation primarily filtering out low energies.

The intensity of the radiation also decreases inversely proportional to the distance from the source focus to the measurement point.

The absorbed dose in a material per unit of time depends on the energy of the incident radiation, its intensity, and the type and structure of the material. In general, it can be said that for the same energy and intensity of the incident radiation, denser bodies absorb more, and, in addition, the material with a higher effective atomic number absorbs more.

The calculation of the effective atomic number and the mass attenuation coefficients of the material remain beyond the objectives of this preliminary study.

The corrected for the time measured absorbed dose along the central line of the beam with the detector placed in front of the armor plate (Din) and behind the armor plate (Dout), for a ballistic plate with protection level IV, are presented in Fig 2.

The absorbed dose rate at the entrance of the ballistic plate increases but not linearly because it also depends on the filtration which is also a function of energy. The dose rate at the exit of the armor plate also increases with increasing radiation energy but more slowly due to the absorption and scattering of radiation in the material.

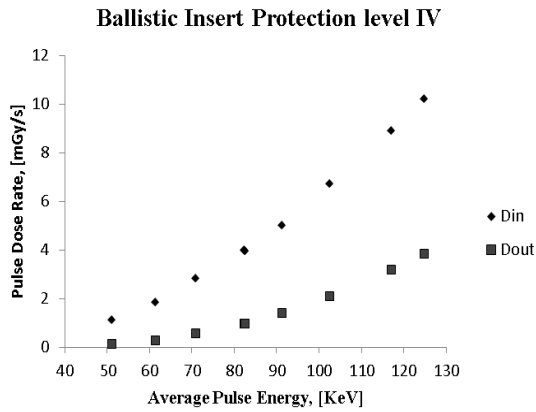


Fig.2. Measured time normalized dose on and below the ballistic slab with protection level IV.

Fig.3 shows the increase in absorbed dose in the armor plate material as a function of incident radiation energy.

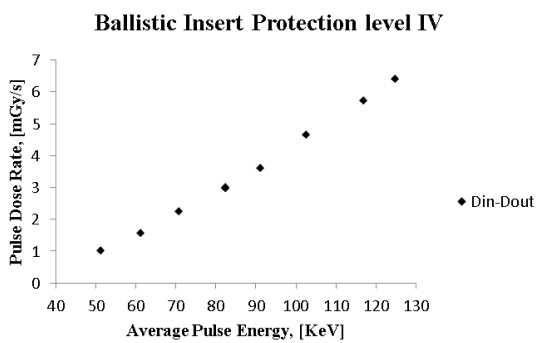


Fig.3. Calculated time-normalized absorbed dose in a ballistic plate with protection level IV.

In Fig. 4 we have shown the calculated attenuation values of the radiation passing through the armor plate material as a function of the incident radiation energy, other things being equal. It can be seen that at low energies we have more protection.

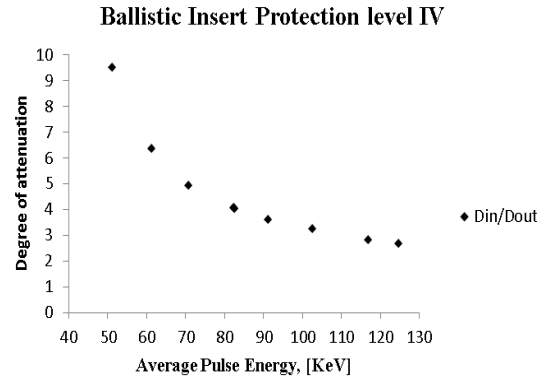


Fig.4. The calculated degree of attenuation of radiation energy passed through a ballistic plate with protection level IV.

Fig. 5 shows the comparison of the attenuation rate of passed radiation from ballistic plates with different degrees of ballistic protection. The attenuation rates for two different energies are indicated on the graph.

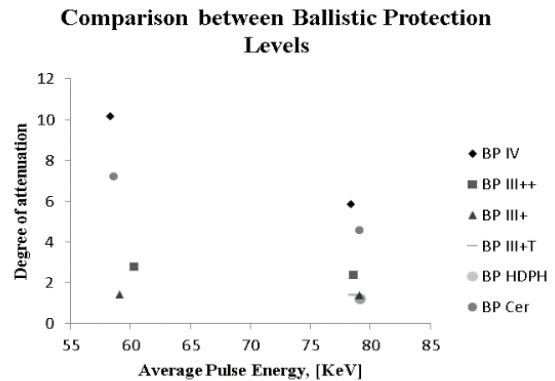


Fig.5. Comparison between attenuation values for ballistic plates with different levels of protection.

It is interesting to note the coincidence of the values of four test plates at 80 keV. Armour plate 6 retains its attenuation rate value despite the post-ballistic test structural damage.

Fig.6 shows an X-ray image of test plate 6, it can be seen that the structural damage of the plate material is localized in an area close to the point of impact and the overall homogeneity of the plate is preserved.

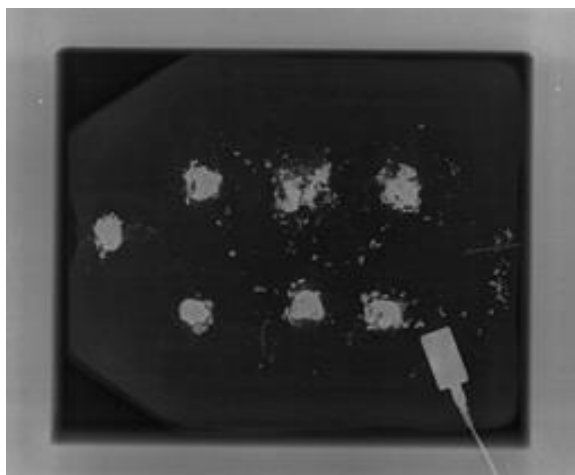


Fig. 6. shows an X-ray image of test plate 6.

Fig. 7 shows the dependence of the attenuation as a function of the incident radiation intensity for a pulse interval of 100 ms and an energy of 80 keV. The radiation intensity is represented by the magnitude of the pulse charge which is the product of the magnitude of the current and the pulse time. It can be seen that the variation is less than 0.02 and practically the degree of attenuation does not depend on the intensity in these intensity ranges.

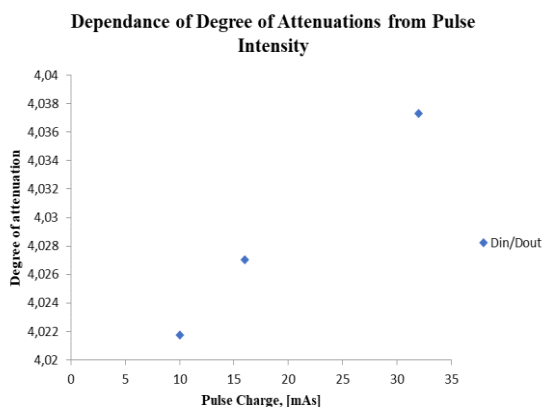


Fig. 7. Degree of attenuation as a function of the incident radiation intensity for a pulse interval of 100 ms and an energy of 80 keV.

#### CONCLUSIONS

To the best of the authors' knowledge, results on photon radiation attenuation in this energy range from ballistic panels are presented for the first time. Thus, the obtained original results will allow us to model the degree

of protection in various hypothetical situations with various complex spatial configurations [8], as well as to assess the harmful effects of photon radiation on servicemen. Having these estimates, it will be possible to modify the action plans to maximally protect personnel operating in environments with increased radiation hazards.

The data obtained in the study will help to design a more thorough study of various ballistic materials.

#### ACKNOWLEDGMENTS

This work 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. The authors are grateful to the company MARS ARMOUR for providing hard armor samples.

#### REFERENCES

- [1] H. Theodore Harcke et al., *Imaging Body Armor*. Belmont, CA: Wadsworth, 1993, pp. 123-135. *Military Medicine*, Volume 167, Issue 4, April 2002, Pages 267–271.
- [2] Y. Karabul, "Ionizing Radiation Shielding Properties of Tantalum Pentoxide Doped High-Density Polyethylene Composites: A Theoretical Study". *Journal of Engineering Technology and Applied Sciences* 8 (3) 2023 : 143-154.
- [3] Plamen Tashkov, "Ballistic impact study on textile structures". Sophia: Defence Advanced Research Institute. 2002.
- [4] B. Genov, Nikolov N. V., G. Genov, Development of ballistic methods for ballistic protection testing, MNC "CHEMUS 2006", collection. tr., 2006, ISSN: 1312-2916 (print), p. 329-337.
- [5] Yna Dimitrova, "Analytical model for examination of shots grouping alteration in single fire shooting", International scientific conference "Defense Technology Forum 2023", Shumen 2023, c. 355-358, ISSN 2815-4274.
- [6] Ballistic Resistance of Personal Body Armor. NIJ Standard–0101.04. Available: <https://nij.ojp.gov/library/publications/ballistic-resistance-personal-body-armor-nij-standard-010104>
- [7] "Handbook of basic quality control tests for diagnostic radiology", IAEA Human Health Series No. 47, International Atomic Energy Agency, Vienna, 2023.
- [8] D. Dimitrov, "Analytical model of the geometric image of targets with complex spatial configuration", Scientific Session with International Participation, VVUAPVO "P.Volov", Proceedings, Shumen, 2001; Proceedings Part II, pp. 111 - 116, Shumen, 2002 ISBN 954-9681-02-3.
- [9] Radcal Corporation. Available: <https://radcal.com/>
- [10] SOFIMAE. Available: <https://www.sofimae.fr/>
- [11] MARS Armor, "MARS Armor Catalog. Armor Hard Armor", 2230 Kostinbrod, Bulgaria, 2 Poletto, Industrial Zone. Available: <https://www.marsarmor.com>.

# Research on the change in ballistic characteristics of ammunition with a modified projectile shape during its movement in an air environment

Rosen Lazarov

Department of „Armament and Technology for Design“  
National Military University “Vasil Levski”  
Shumen, Bulgaria  
poceh\_69@abv.bg

**Abstract.** When changing the shape of a projectile in order to reduce its ricochet effect when encountering a water environment, its ballistic characteristics during its movement in the air are also altered, such as projectile speed, range, ballistic coefficient, and shooting grouping. The present study aims to determine the influence on the projectile's speed and ballistic coefficient of the radial rings made on its ogive part.

**Keywords:** external ballistics, form factor, ballistic coefficient, modified projectile.

## I. INTRODUCTION

Changing the shape of the projectile causes changes in its ballistic characteristics: projectile velocity, ballistic coefficient, grouping of shots, and air resistance force. The impact of changing the projectile's shape on the average point of impact is presented in [1].

The ballistic coefficient (BC) allows for the determination of the trajectory and the analysis of other ballistic characteristics of the projectile. The value of BC is provided by ammunition manufacturers on the boxes and in the ammunition manuals, as well as on the company's website. Due to manufacturing deviations in the dimensions and mass of the projectiles, as well as differences in atmospheric conditions during experimental

shootings, the value of BC is inaccurate. This inaccuracy turns into an error and makes any analysis based on the external ballistic characteristics of the projectile with this BC inaccurate. Having an accurately determined BC is extremely important for conducting a correct external ballistic analysis.

## II. MATERIALS AND METHODS

The subject of the study is a standard projectile of ammunition with the nomenclature number 7.62x54mm, as well as five modified projectile models with radial-slotted channels on the ogive part, shown in Fig. 1, and with the number and setback of the channels from the tip indicated in Table 1.

The study is conducted following the methodology outlined in [2]

The required minimum number of experimental data in the series is determined according to the methodology from [3], [4] which was also used in [5].

TABLE 1 THE MODELS

№	Name of the model	Distance of the channel from the tip of the projectile (mm)	
		First	Second
1.	Model 1		
2.	Model 2	3	
3.	Model 3	3	6,4

Print ISSN 1691-5402  
Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8194>

© 2024 Rosen Lazarov. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

4.	Model 4	6,4	
5.	Model 5	12,7	
6.	Model 6	3	12,7

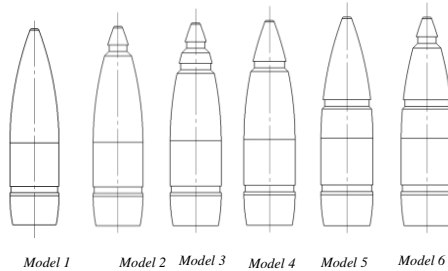


Fig. 1 The models of ammunition used in the experiment  
 1. Model 1 – Projectile with unchanged shape,  
 2. Model 2 – Projectile with one channel, located 3 mm from the tip,  
 3. Model 3 – Projectile with two channels, located 3 mm and 6.4 mm from the tip,  
 4. Model 4 – Projectile with one channel, located 6.4 mm from the tip,  
 5. Model 5 – Projectile with one channel, located 12.7 mm from the tip,  
 6. Model 6 – Projectile with two channels, located 3 mm and 12.7 mm from the tip.

For the conduct of the study, a ballistic barrel mounted on a stand (Fig. 2) and leveled with a precision level is used. Series of 20 shots from each model are fired. The velocity of the projectile is measured at 25 m from the muzzle end of the ballistic barrel using the Drello bal 4040 speed measuring device [2].



Fig. 2 A stand with a ballistic barrel mounted on it and secured to a foundation.

The ballistic coefficient is determined by the formula (1) [6], [7], [8]:

$$BC = \frac{id^2}{m} \quad (1)$$

where:

- i – shape factor of the projectile;
- d – caliber of the projectile (mm);
- m – mass of the projectile (g).

The shape factor of the projectile allows for the calculation of the ballistic coefficient for each individual model and is determined by formula (2) [9]:

$$i = \frac{R}{R_{st}} \quad (2)$$

where:

R – resistance force of the projectile with a modified frontal part;

$R_{st}$  - resistance force of a standard projectile.

The components of the air resistance force that affect the flight of the projectile are:

- Front part resistance.

When moving through the air, the projectile displaces air to the sides. A part of the kinetic energy of the bullet is used to displace the air. This loss of energy is due to air resistance and causes a constant decrease in the velocity of the bullet. The compression of the air created by the nose of the projectile spreads through space as a pressure wave and creates a disturbance that moves through space at the speed of sound. When the projectile moves at a speed less than the speed of sound (less than 340 m/s), the waves move ahead of the projectile and spread far from it (Fig. 3).

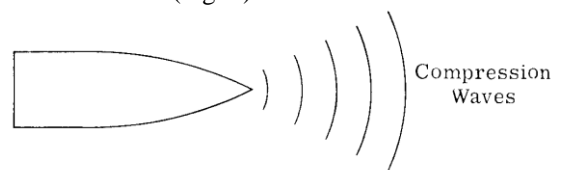


Fig. 3 Pressure waves created by the movement of a projectile in an air medium at subsonic speed [10].

The resistance of the front part increases significantly at projectile speeds above the speed of sound. Then, the compression waves cannot propagate far from the projectile, as it moves faster. They accumulate into a shock wave at the nose of the projectile (Fig. 4).

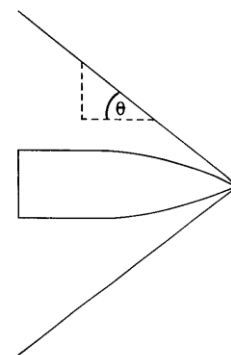


Fig. 4 Shock wave created by the movement of a projectile in an air medium at supersonic speed [10].

- Base resistance.

Turbulence is created behind the projectile, causing additional resistance. The reason is a low-pressure zone immediately behind the projectile, which occurs because the air cannot return quickly enough behind the projectile (Fig. 5). The result is a vacuum, which manifests as resistance to motion.

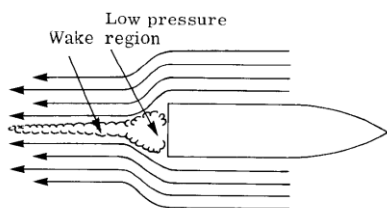


Fig. 5 Turbulence created behind the projectile [10].

- Surface resistance.

Additional resistance during motion is manifested by the air adjacent to the surface of the projectile. The air moves along the surface at the velocity of the projectile. Due to internal friction, the next layer of air particles also begins to move, but at a slower speed.

This layer imparts motion to the next, with each successive layer reducing its speed. Achieving a higher roughness class in the manufacturing of the projectile reduces surface resistance [10].

- Resistance of protuberances.

The resistance of protuberances is caused by the protrusions on the body of the projectile. This component of the air resistance force can be greatly reduced by removing the protrusions on the body of the projectile, and those that cannot be removed should be properly designed [10].

The air resistance force can be determined by the measured velocities with formula (3) [9]:

$$R_{cp} = \frac{q \cdot v_1^2 - v_2^2}{2g \cdot L} \quad [N] \quad (3)$$

where:

q – gravitational force on the projectile (N);

g – acceleration due to gravity (9,81 m/s<sup>2</sup>);

L – distance between the velocity measurement points (m);

v<sub>1</sub> – initial velocity of the projectile (855 m/s) [11];

v<sub>2</sub> – velocity of the projectile, measured at a distance L (m/s) [12].

### III. THE RESULTS

The velocities of the different projectile models, measured at a distance of 25 m, are indicated in Table 2 [12].

Table 2 THE VELOCITIES

Ammunition /type/, batch	7,62 x 54 mm ammunition Γ 13-80-10					
Air temperature	15°C					
Charge temperature	18°C					
Number of the model	0	1	2	3	4	5
Measured velocity at 25 m V <sub>25</sub> [m/s]	828	826	824	827	816	811

The values of the air resistance force for each individual model from the experiment are given in

Table 3 based on calculations according to formula (3).

Table 3 THE VALUES OF THE AIR RESISTANCE FORCE

№	The name of the model	Resistance force R <sub>cp</sub> (N)
1.	Model 1	8,724672
2.	Model 2	9,311437292
3.	Model 3	9,876144205
4.	Model 4	8,983057602
5.	Model 5	12,42824248
6.	Model 6	13,90691601

After substituting the values of the air resistance force into formula (2), we obtain the values for the shape factor of the projectile (i) for each model in the experiment. The results are presented in Table 4.

Table 4. THE VALUES OF THE SHAPE FACTOR OF THE PROJECTILE

№	The name of the model	Shape factor of the projectile i
1.	Model 1	1
2.	Model 2	1,067253565
3.	Model 3	1,131978853
4.	Model 4	1,029615509
5.	Model 5	1,42449395
6.	Model 6	1,593975797

When calculating the BC, the same mass value for the projectile cannot be used due to the material removed to create the channels in the ogive part. The mass of the standard projectile is 9.6 g [13], and for each model of modified projectiles, the mass will be reduced by the amount of material calculated to have been removed in the creation of the radial channels [10]. The mass of the projectile for the respective model is given in Table 5.

Table 5 THE MASS OF THE PROJECTILE

№	The name of the model	Mass of the removed material (g)	Total mass of the projectile (g)
1.	Model 1	0	9.6
2.	Model 2	0,049612	9,550388
3.	Model 3	0,1126475	9,4873525
4.	Model 4	0,0630355	9,5369645
5.	Model 5	0,0646055	9,5353945
6.	Model 6	0,1142175	9,4857825

After all the components necessary for determining the BC have been calculated, they are applied in formula (1). The results are presented in Table 6

Table 6 THE RESULTS OF THE BC

№	The name of the model	Balistic coefficient (mm <sup>2</sup> /g)
1.	Model 1	6,534
2.	Model 2	6,973435
3.	Model 3	7,39635
4.	Model 4	6,727508
5.	Model 5	9,307643
6.	Model 6	10,41504

#### IV THE CONCLUSION

The calculated ballistic coefficient for the modified ammunition is smallest for Model 4 (with one radial channel located 6.4 mm from the tip of the projectile) and is very close to that of the standard projectile. This indicates that, aerodynamically, this projectile has characteristics most similar to the standard projectile. On the other hand, a projectile with the same channel distance, made on the ogive part, showed the best angle for forming a cavitation cavity when encountering a water medium [14]. The creation of such a cavity leads to a reduction in the projectile's ricochets from a water medium. Thus, the projectile from Model 3 has both limited ricochet action and good aerodynamic qualities.

#### ACKNOWLEDGMENTS



The report is being carried out under the National Scientific Program "Security and Defense", adopted by Council of Ministers Decree № 731 of October 21, 2021, and in accordance with Agreement № D01-74/19.05.2022.

#### REFERENCES

1. К. Калев, Р. Лазаров, Изследване на изменението на координатите на средната точка на попаденията при стрелба с куршуми с радиални изрези върху оживалната част, Международна научна конференция „Отбранителни технологии” - 2022 г., НВУ „Васил Левски“, факултет „Артилерия, ПВО и КИС“, ISSN 2367-7902, (pp. 304-308)
2. В. Ганев, Р. Лазаров, Я. Димитрова, Б. Банков, Полигонни изпитвания на промяната на балистичните характеристики на боеприпаси с изменена форма на проектила при срещата му със среда с различна плътност, Международна научна конференция „Отбранителни технологии” - 2023 г., НВУ „Васил Левски“, факултет „Артилерия, ПВО и КИС“, ISSN 2367-7902,
3. Я. Димитрова, Изследване на влиянието на трибологичните характеристики на шумозаглушителя върху групираността при стрелба със стрелково оръжие, Дисертационен труд, НВУ „В. Левски“, Факултет „Артилерия, ПВО и КИС“, Шумен 2021 г. (pp.109-110)
4. V. Ganev and Ya. Dimitrova, “Determination of change of the point of the fire shots at shooting with fitted chamber type suppressor” - International scientific conference CONFSEC, year 1, issue 3, Borovec 2017 ISSN (print) 2603-2945, ISSN (online) 2603-2953 (pp. 129-132)
5. В. Ганев, Р. Лазаров, Я. Димитрова, Б. Банков, „Анализ на възможностите за промяна формата на куршума на боеприпас 7,62x54 с цел намаляване на рикошетното му действие при среща с водна среда“ – Научна конференция „Логистиката и обществените системи” – 2023 г., ИК на НВУ „Васил Левски” – ВТ, ISSN 2738-8042, (pp. 181-186)
6. Шапиро, Я., Внешняя баллистика, Государственное издательство оборонной промышленности, Москва 1946 г. (pp. 57-61)
7. B. Litz, Applied Ballistics For Long Range Shooting, Third edition, ISBN 978-0-9909206-1-8 (pp. 15-39)
8. П. Верещагин, Массовые, динамические характеристики и внешняя баллистика снарядов – pp. 17
9. И. Балагански, Основы баллистики и аэродинамики, Издательство на Новосибирский государственный технический университет, 2017. – 200 с., ISBN 978-5-7782-3412-3, (pp. 140 - 145)
10. C Farrar and D Leeming, Basic Military Ballistics- ISBN 0-08-028342-X (Hardcover), ISBN 0-08-028343-8 (Flexicover) (pp. 73-77)
11. Наставление по стрелково дело. Материална част на стрелковото оръжие, Военно издателство, София, 1987 г. (pp. 428)
12. Р. Лазаров, Изследване на влиянието на формата на куршума върху рикошетното му действие, Дисертационен труд, НВУ „Васил Левски“, факултет „Артилерия, ПВО и КИС“, Шумен 2022 г.
13. Е. Тихонов, Боеприпасы к ручному стрелковому оружию (пособие для экспертов), Министерство юстиции СССР, Москва 1976 г. (pp. 22)
14. В. Ганев, Б. Банков, „Изследване на движението на проектил на боеприпас 7.62x54 във водна среда“, Научна конференция „Актуални проблеми на сигурността”, Велико Търново 2023 г, ISSN 2367-7473, pp.1511 – 1516.

# *Contemporary challenges to the protection of the country's sovereignty*

**Rumen Marinov**  
*Security and Defense Faculty  
Vasil Levski National Military  
University  
Veliko Tarnovo, Republic of  
Bulgaria  
ramarinoff@gmail.com*

**Abstract.** In the present study, security is considered a category related to the protection of the national sovereignty and interests of the country. Today, we live in an international environment, and politics and security are closely intertwined. The law of international relations regulates relations between states and defines their rights and obligations in many areas, including trade, environmental protection, human rights, and peaceful coexistence. The principle of sovereignty is one of the most fundamental principles of international law. Therefore, each country is entitled to govern its territory and people without interference from other countries. The paper discusses how international law and sovereignty contribute to maintaining international order, security, and cooperation. International law not only provides a framework for resolving conflicts between states but also mechanisms for promoting international cooperation on a broad range of issues. It also provides a framework for the peaceful settlement of conflicts and protects vulnerable groups such as refugees and displaced persons. Are you aware of the contemporary challenges that threaten to protect our country's sovereignty? It's a crucial issue that needs our attention. Let's understand the challenges we face in protecting our nation's sovereignty.

**Keywords:** *international environment, international law politics, security, sovereignty*

## I. INTRODUCTION

In the world, dynamic events and complex relationships dictate events. Inevitably, states and their politics, security, and the international environment become key elements in the formation of global stability and cooperation. Concepts such as sovereignty and international law play an important role in this context, defining the framework in which relations between states develop. "...commentary on security's changing nature in a world of COVID-19 often overlooks the reality that traditional hard security challenges requiring military power – and its lucid assessment – are unlikely to diminish, and may even be exacerbated [1].

## II. MATERIALS AND METHODS

The interrelationships between politics, security, the international environment, international law, and sovereignty are synthesized. Models are explored in which nation-states strike a balance between protecting their interests and inspiring solid cooperation for the common good of the world. The significance of the understanding that in the modern world borders and interdependencies merge into one inseparable reality is emphasized. The study is supplemented with two figures that illustrate the important analytical estimates.

## III. RESULTS AND DISCUSSION

Politics, as an ambiguous term, reflects the striving of states to achieve specific goals and manage internal and external relations. It interacts continuously with security as the main element for protecting national interests against internal and external threats. At the same time, the international environment serves as a platform on which states express their strategies, develop relationships, and seek common solutions to global security challenges. This represents a parallel to "...contemporary challenges and the corresponding response to achieve organizational effectiveness...[2]. This cooperation requires compliance with the principles of international law, which serves as a foundation for justice, peace, and cooperation between sovereign states. In this context, the notion of sovereignty emerges as a fundamental principle in political theory and practice. Sovereignty refers to the authority and control that a nation or state exercises over its territory, people, and resources. It encompasses the state's ability to make independent decisions and protect itself from external interference. Sovereignty is the inalienable basis of its independence and ability to formulate policy and ensure its security on a global scale.

In this complex context of politics, security, international environment, international law, and sovereignty, nation-states seek a balance that ensures not only the protection of their interests but also sustainable cooperation for the common good in a world where borders and interdependencies merge into one inseparable reality.

*Print ISSN 1691-5402  
Online ISSN 2256-070X*

<https://doi.org/10.17770/etr2024vol4.8187>

© 2024 Rumen Marinov. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)



In turn, security is a category related to the state and is the subject of the present study. This category has the greatest scholarly achievements in the field of political science, given that the field of international relations has studied and gathered knowledge about relations between states. Following the theories developed by these sciences, the military security of the state is mainly due to the existence of the subject, the state, and the international environment that surrounds it. The state and the international security environment are closely related and interdependent. The state, as an actor on the international stage, interacts with other states, governmental, non-governmental, and international organizations in the international environment that determines security and its interests. When the state is in constant interaction with other states and actors in the international environment, which may pose a threat to its security, we call it external threats. The responsibility for overall coordination is critical to neutralizing the threat level is... [3]. In this regard, the effort of a state to use its foreign policy and diplomacy to focus relations with other states in a certain direction and to protect its interests is called international politics and diplomacy. This may include maintaining military alliances, signing security agreements, participating in international organizations, negotiating deals, etc. The state then obeys the rules and norms of international law that regulate the behaviour of states in the international environment. Governance and strategy imperatives are changing at a rapid pace. This gives rise to gaps in public international law in various areas. It fails to compensate for the development of state practice and the emergence of factors and technologies that were not anticipated by the existing law. Gaps or outdated provisions in many treaties and within international law are primarily where there are no agreed rules to govern state actions that in turn affect other states and their populations. Some of the areas where legal norms could be expanded or updated include: the use of force by states; operations against non-state actors; refugee protection, and cyber security. States address these gaps in different ways.

Next, we will discuss international cooperation. Analyses of the last five years indicate that, for various reasons, the alliance structures in the key strategic regions of the world – Europe, the Middle East, and the Indo-Pacific region – are changing. The US is taking several steps to strengthen its presence there. At the end of 2017, the United States launched an idea to transform the American Pacific Command. Half a year later ...on May 30, 2018, the US Secretary of State for Defence announced the transformation of the US Pacific Command into the Indo-Pacific [4]. A few days later, during the conference in Singapore, the Minister of Defence of the United States, Lloyd Austin made further clarifications about the idea of the Indo-Pacific region, emphasizing precisely the aspects of regional security. For the next three years, the US maintained that it did not plan to create an “Asian analogue of NATO” aimed at China. Their latest diplomatic moves suggest the opposite. In October 2021, a political and trade-economic association was established with the participation of Israel, India, the USA, and the UAE called I2U2. As a natural continuation of this process, in January 2022 the Foreign and Defence Ministers of the United States and Japan after negotiations, in the “2+2” format, emphasized that they “welcome the growing engagement with the issues of the Indo-Pacific region of the European partners and allies”. In this context, the EU, NATO, and the tripartite quasi-alliance AUKUS created in 2021 are explicitly mentioned. Here we could conclude that the internal and external interests and relations of NATO and the EU outside Europe are growing. Two more facts that are eloquent enough. In early 2022, Saudi Arabia restored relations with Iran after signing an agreement. China was the mediator between the two countries. At the same time, Russian capital moves freely between India and the UAE. Certainly, the US wants to impose sanctions on Abu Dhabi, but that would jeopardize the future of I2U2. The strategic goal of the US in creating the association is to cooperate with the Middle East, South Asia, and the Americas so that they can advance their economic technology and diplomacy. At the same time, the

political relations between Japan and India in the modern era are not to be underestimated, and they date back more than 70 years. Economic and diplomatic ties between the two sovereign nations strengthened significantly in 2000 after the signing of the “Japan-India Global Partnership”. The deteriorating security environment in the Indo-Pacific region has also reinforced the need for increased interoperability between NATO and Japan. At the same time, through the long-standing alliance with the US and increased cooperation with European countries, a closer integration is achieved between the national defence industrial bases, which are organized both according to the doctrinal basis and operational policies.

In continuation of the analysed geostrategic processes, we can point out as indicative of the relations of the EU and the decisions of the European Council from October 2023 regarding Israel and the development of the situation in the Middle East, both in the region and beyond. ...The European Council again condemns Hamas in the strongest possible terms for its brutal and unabashed terrorist attacks in Israel [5]. International institutions are raising doubts about their inability to adapt to the intensifying competition between the great powers. At the same time, rising and resurgent powers around the world are racing to assert the strategic self-determination of their regions.

It is also important to consider the global aspects of the security environment [6]. They cover a wide range of challenges and threats that affect international security. All these factors are common to different countries and can have a significant impact on international relations and stability. Military security is inextricably linked to the existence of the armed forces. These are the main elements belonging to a category of neorealist theories of international politics concerned with the possibilities of survival and growth of states. As a result of the efforts that countries make to ensure the security of their military forces, it is obvious that the existence of security problems will significantly affect the security of the country's military forces in terms of their ability to maintain security for their military forces. In practice, countries create increased uncertainty among themselves, as each country interprets its actions as defensive and those of the others as potentially threatening, regardless of the reasons for an action. The sources of military threats must be considered within the framework of the characteristics of the international environment, in which military power is among the main ones for states and international politics.

This is because a military instrument can be used to physically destroy elements of another country as well as use effective and efficient force to destroy elements of another country. It is well known that this power is a very effective method of influencing the policies of other countries; it also poses a threat to their security as a result of its very existence. This threat is exacerbated by the existence of states whose international relations are based on dishonesty. Currently, the development of military technology is leading to rapid changes in relations between countries. This will inevitably lead to ...the development of information technology and its ever-wider implementation and use in all spheres of security and defence increases the degree of threats from illegal actions...[7]. In other words, the effect of the developing military strategies and the development of information and communication technologies will intensify the effect of the changing nature of conflicts. This presents the prospect of rogue states defeating other states unfairly but successfully. A country that realizes this fact, when forming alliances and signing arms control agreements, shows caution and actively tries to ensure its security. It is clear to all of us that military power, by its very existence, poses a threat to the security of other countries. This is a circumstance that many authors of official international documents overlook.

Furthermore, it is important to note that security refers to the most dangerous consequences of determination/fear. An attack on the sovereignty or territorial integrity of a country by the military can pose a serious threat. As a result of the potential

risks associated with military conflict, it is vital that a nation's sovereignty and territorial integrity are protected. In general, governments are wary of taking excessive risks as the loss of sovereignty and territorial integrity can have serious and long-term consequences. Diplomacy, negotiation, and peaceful dispute resolution are often emphasized to prevent military conflict and protect sovereignty. Preserving sovereignty and territorial integrity requires building and maintaining stable relations with other countries as well as supporting rules and norms in the international community. When Israelis and Palestinians, Russians and Ukrainians, Kurds and Turks compete for the favour of global public opinion, they all use the same arguments about human rights, state sovereignty, and international law [8]. This is, in effect, playing on people's fears. Here is what Karl Marx said about fear: "Cruelty is characteristic of laws dictated by fear because fear can only be energized by being cruel."

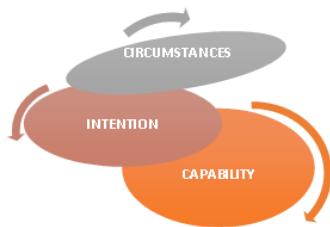


Fig. 1. Potentially dangerous conditions for a country to start a military conflict

The **first factor** of potentially dangerous conditions for the state is **"capability"** (Fig. 1). It refers to the physical ability to wage a large-scale military conflict. We cannot as a feature of this factor that every sovereign state, except perhaps the smallest ones, has the ability to conduct a military conflict on a large scale. While maintaining the balance of power, the action of the "capability" factor need not cause serious harm to another state. However, most countries have to consider the possibility of direct threats coming from their neighbors. Also, a state with relatively long maritime borders must take into account the fact that a state that is not an immediate neighbour may also pose a threat to its territory. The situation is further complicated by the possibility of airstrikes, which can be carried out even by not-so-nearby countries.

The **second factor** of potentially dangerous conditions for the state is **"intention"** (Fig. 1). It refers to the degree of determination of the need for a country to initiate a military conflict or war. It is necessary to consider the question of defence and especially its definition. Some researchers see it as the protection of territory and sovereignty, and others, in a broader sense, as the protection of national interests.

An example of the protection of the country can be found in the Bulgarian Constitution, which states that: Article 9 (1)...The armed forces guarantee the sovereignty, security, and independence of the country and protect its territorial integrity. (2)...The activities of the armed forces shall be regulated by law [9].

An example of a narrow interpretation of the protection can be found in the Polish constitution, which states that: 1. The Armed Forces of the Republic of Poland serve to protect the independence of the state and the indivisibility of its territory and guarantee the security and inviolability of its borders [10].

This essentially means that the armed forces of the Republic of Bulgaria and the Republic of Poland will preserve the independence and integrity of their territory and guarantee the security and integrity of their borders. In contrast to the cited constitutions, the constitution of the Czech Republic states that:

Article 39...(3) Adoption of a resolution on the declaration of war and adoption of a resolution on consent to the deployment of the armed forces of the Czech Republic outside the territory of the Czech Republic or to the residence of the armed forces of other countries on the territory of the Czech Republic, as well as of the adoption of a resolution on the participation of the Czech Republic in the defense systems of an international organization of which the Czech Republic is a member, with the consent of an absolute majority of all deputies and an absolute majority of all senators [11].

Here, as can be clearly seen, there is no express text regulating the activities of the armed forces in defence of the country's sovereignty and territorial integrity, but the declaration of war is regulated.

The third country subject to our research is Germany and its Basic Law for the Federal Republic of Germany. It states:

Article 87a ...(2) With the exception of defence, the armed forces may be used only insofar as authorization is expressly stated in this Basic Law [12].

In contrast to the other two constitutions in the FRG, the functions of the armed forces are expanded, with them having responsibilities for internal order and security in support of other bodies to guarantee the country's sovereignty.

If we look at the **"intention"** factor in our south-eastern neighbour the Republic of Turkey, we will see that in their supreme document – the constitution of the Republic of Turkey, it is written:

Article 92 – The power to authorize the declaration of a state of war in considered legal cases and except when required by international treaties to which Turkey is a party to the treaty or by the rules of international law to send Turkish armed forces to foreign countries and to allow foreign armed forces to be stationed in Turkey is a decision of the Grand National Assembly of Turkey. If the country is subjected to sudden armed aggression while the Turkish Grand National Assembly is adjourned or interrupted, and thus it becomes imperative to decide immediately whether to use the armed forces, the President of the Republic may decide to use the Turkish armed forces [13].

A minimal but significant difference with other constitutions is noticeable here. The decision to declare war is within the competence of the Grand National Assembly or the Grand National Turkish Assembly of Turkey with one significant exception that does not exist in the other cited documents. The president of the republic can unilaterally decide on the use of the Turkish armed forces under the conditions specified in the quoted article of the constitution.

Alternatively, many countries that have national interests beyond their borders assign their armed forces to protect those interests wherever they are located and based on their government's requirements. Likely, the use of armed forces is primarily driven by the need to support a state's national interests rather than its sovereignty and territorial integrity. It is important to note that, given that states use the term "security" to denote the preservation of what they consider to be their vital interests, it has a defensive connotation only in the sense that any nation is prepared to use force, to protect those interests. A country's activities on the international stage can be considered defensive or international depending on the definition of the concept of balance of power. However, the actions have a defensive nature *ipso facto* – they are aimed at protecting its vital interests.

In light of these considerations and the analysis made, it is now possible to determine the fundamental nature of military security. There is no doubt that this is a category that should be

directly related to the concept of security. Based on a predetermined understanding of state security, we must recognize that military security is a state that is transitory in time. At the same time, it specifies the ability of the state to satisfy the needs of people to exist and develop, regardless of the presence of real or potential military risks and threats. Similarly, the concept of balance of power encompasses the awareness of the situation in question as well as all activities aimed at achieving the desired level of security.

Particularly characteristic of the second potentially dangerous condition for the state is the “**intention**” factor, which also contains three main components of security. They are:

1. variable condition over time;
2. awareness of changing conditions of security over time;
3. activity aimed at achieving the desired condition level.

The specified elements defining potentially dangerous security conditions (1-3) are presented in Fig.2:

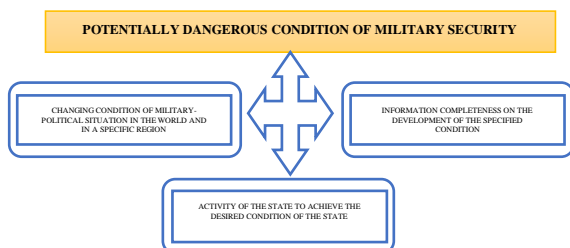


Fig. 1 Content of a potentially dangerous condition of the military security component

The first component, the **changing condition of the military-political situation** related to military security refers to the impact of various interested countries as well as environmental factors that affect the military sphere. In turn, this affects the state's ability to meet the social needs associated with their existence and development. Therefore, military security exists during the successive actions of the states (conditions) resulting from the activity of the subject of security. This is independent of changes in the activity of the object's environment.

The second component is **awareness of the changing condition of security** over time. The fact that military security conditions are changing and that these changes depend on many factors shows that security is also a process. This means that it is necessary to carry out the activity leading to the desired effect. This effect is also the result of factors other than one's own activity. Military security actors seek to minimize the effects of factors other than their own activities. They usually actively seek to shape as much of their environment as possible. Therefore, we can assume that the main part of the military security of the state is a function of its activity.

The third component **activities aimed at achieving the desired condition**. Due to the described characteristics of the international environment as well as the ambition of states to secure their own interests, each state strives for a high level of military security. Therefore, continuous activity of the relevant authorities to maintain military security is necessary to maintain the desired level of security.

This raises the question of a model of the national security system that maintains the level of military security. The importance of this issue stems from the fact that the structure of such a model and its implementation have a direct impact on the level of military security. If the general model aims to achieve a better condition of military security, we get the following:

1. activities to achieve and maintain situational awareness;
2. standards for neutralizing military threats, especially military attacks.

Security within the national critical infrastructure system is interpreted as a dynamic balance between potential threats and measures for protection against them [14]. While looking for the elements of a national security system model, we should note that most models contain a **module for control, an activity module, and an operational module**. Their existence depends on basic assumptions of praxeology or management theory.

The first essential element of an existing national security system to maintain the desired level of military security is to have a management module. It is a system component that aims to manage, coordinate, and control certain functionalities and/or processes. Activities aimed at preventing military threats must be integrated into the other activities of the state. They should also remain within applicable national and international law and disclose their effectiveness as well as many other characteristics. This activity usually takes place under various constraints, the most important one today being the *level of public support*.

We can emphasize that the basis of any reasonable activity is awareness of the situation in which the object is located. This awareness is essential to making sound decisions about taking action. Therefore, this awareness shapes the decisions that are made. These decisions are directly imposed on the management of the subject's activities. When military security is the focus, an important part of this awareness is knowledge of military risks and threats, particularly the military capabilities and intentions of the adversary or adversaries. It is worth noting that the efficiency of the system depends on its components and the processes taking place in it as well as on the interaction and influence of the environment [15].

The **third factor** of potentially dangerous conditions is “**circumstances**” (Fig. 1). This is how F.H. Hartmann defines circumstances: “This knowledge is the result of considerable effort undertaken by the state to reveal an aspect which its opponent is diligently trying to conceal, i.e. the capabilities and intentions of its armed forces. Without this knowledge, the state is unable to properly assess military threats and thus choose appropriate countermeasures. Therefore, it must be assumed that one of the main elements of the activity model system necessary to maintain the desired level of military security is its information module [16].

During a war, the strategy defines the main goal and objectives, the plans and methods for achieving it.

The strategy gives a meaningful character to the goals and means and defines the possibilities, potentially dangerous circumstances, and chances of victory. An important place is occupied by the so-called “**geographic zones**”, which have a strong influence on the strategy, geopolitical and geostrategic factors.

Conditions such as terrorism, cyber-attacks, and the proliferation of nuclear or biological weapons are examples of conditions that can be dangerous (threats) to state security. In addition to government organisations, non-governmental organisations can also produce them. There is also the possibility of violating international agreements and disputes with other countries, which can lead to potentially dangerous situations (threats) for the country's security. A state's behaviour and outcomes are influenced by the international environment, whereby the actions of actors in that environment can be indirectly influenced by states. This means that the military actions of one country can pose a potential danger to another country and can negatively affect a number of aspects of that nation. This example provides a simplified model of how military security can be maintained by following the most important elements of the model.

The strategic approach to problem-solving is ultimately pragmatic. There is nothing more important than strategy if one is to succeed in what one is trying to achieve. Strategists ask the same important question as those who deal with other aspects of

politics: Will the idea work under the circumstances in which it will be implemented?

This leads to another significant factor, namely an activity module used to address military threats. The presence of a management module and a situational information acquisition module allows for the acquisition of reliable data on military threats and the environmental situation, which supports making informed decisions about the necessary actions during a crisis. However, it is essential to have an executive module that enables the implementation of planned actions and countering military threats.

The executive sphere in the proposed model reflects the **operational module**. The module is a form of activity aimed at countering detected military threats. Such activity is determined by the individual strategy of the given subject and by the military operations conducted by external authorities. Therefore, military security is a dynamic process through which constant changes take place. These changes depend on the state's defence activity and changes in the environment.

It is necessary to note that participants in international relations, both governmental and non-governmental (non-state) organisations to some extent depend on the surrounding environment. This environment affects their behaviour and performance, whereby a state can indirectly influence the actions taken by actors in an international environment. Therefore, military activity can directly deal with various aspects of another state (or non-state entity) or its surroundings. The proposal contains a simplified model of action carried out to maintain the desired level of military security, covering its most important elements. While as a delivery module, of course, it is not unique enough to be included right now. The derived modules are the main activities of the model and in practice should be supplemented by service and support elements. However, the aim here is to extract the most important elements of military security activity.

#### CONCLUSIONS

In conclusion, we can note that the current challenges to the protection of a country's sovereignty and politics are closely related to the issues of the international security environment. States seek not only to ensure their internal stability but also to assert their security in a global context. In this process, the international security environment plays a key role, and the relationships between different states are formed under the influence of political and economic factors.

Security is considered a category related to the protection of national sovereignty and interests of the country. International law regulates relations between states and defines their rights and obligations in many areas. It also contributes to the maintenance of international order, security, and cooperation by providing a framework for peaceful conflict resolution and protecting vulnerable groups. Politics is the endeavor of states to achieve specific goals and manage internal and external relations. It is in constant interaction with security as the main element for the protection of national interests against internal and external threats. Sovereignty refers to a nation's ability to make independent decisions and protect itself from outside interference. This is the irrevocable basis of its independence.

#### 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] <https://www.iiss.org/research/war-power-rules/> [Accessed: Dec. 28, 2023].
- [2] V.Vasilev, D. Stefanova, C. Popescu, (2023). 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; <https://doi.org/10.1108/978-1-83753-190-520231004>
- [3] Valentin S. Vasilev, Published under licence by IOP Publishing Ltd, [IOP Conference Series: Earth and Environmental Science, Volume 172, 4th International Scientific Conference SEA-CONF 2018 17–19 May 2018, Constanta, Romania](https://doi.org/10.1088/1755-1315/172/1/012013) Citation Valentin S Vasilev 2018 *IOP Conf. Ser.: Earth Environ. Sci.* **172** 012013 DOI 10.1088/1755-1315/172/1/012013, pp 1-10. [Accessed: Febr. 6, 2024]
- [4] <https://geopolitica.eu/2022/200-broy-4-5-2022/3614-geopoliticheskiye-aspekti-na-amerikanskaya-kontseptsiya-za-indo-tihookeanskaya-region> [Accessed: Dec. 01, 2023].
- [5] N. Dimitrov, National security in Bulgaria – is it really a system? Scientific technical union of mechanical engineering industry-4.0. 2019, Vol. 3, Iss. 1 (5), ISSN 2603-2945, pp. 70-73
- [6] European Council conclusions, 26 and 27 October 2023., EUCO 14/23, CO EUR 11 CONCL 5
- [7] Doktrina na Vaorazhenite sili na Republika Bgaria, NP – 01, Izdanie (A), noemvri 2017 r., Sofia 2017, pp.11
- [8] Yuval Noah Harari. 21 Lessons for the 21st Century, Spiegel & Grau, Jonathan Cape, 21 LESSONS FOR THE 21ST CENTURY Copyright © 2018, ISBN 978-198-480-149-4, pp. 103
- [9] Konstitucia na Republika Bgaria, (Obn., DV, br. 56 ot 13.07.1991 r., v sila ot 13.07.1991 r., izm. I dop, br. 12 ot 6.02.2007 r.)
- [10] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Opracowano na podstawie: Dz. U. z 1997 r. Nr 78, poz. 483, z 2001 r. Nr 28, poz. 319, z 2006 r. Nr 200, poz. 1471, z 2009 r, Nr 114, poz. 946.
- [11] Ústava České republiky ze dne 16. prosince 1992, ústavní zákon č. 1/1993 Sb. ve znění ústavního zákona č. 347/1997 Sb., 300/2000 Sb., 448/2001 Sb., 395/2001 Sb., 515/2002 Sb., 319/2009 Sb., 71/2012 Sb. a 98/2013 Sb
- [12] Grundgesetz für die Bundesrepublik Deutschland, vom 23. Mai 1949, zuletzt geändert am 23. Dezember 2014
- [13] Türkiye cumhuriyeti anayasasi, Kanun No.: 2709 Kabul Tarihi: 7.11.1982 Başlangıç (Değişik: 23/7/1995-4121/1 md.), Bu Anayasa; Kurucu Meclis tarafından 18/10/1982'de halkoylamasına sunulmak üzere kabul edilmiş ve 20/10/1982 tarihli ve 17844 sayılı Resmî Gazete'de yayımlanmış; 7/11/1982'de halkoylamasına sunulduktan sonra 9/11/1982 tarihli ve 17863 mükerrer sayılı Resmî Gazete'de yeniden yayımlanmıştır.
- [14] B. Mednikarov, N. Dimitrov, V. Vasilev, Available from: [https://www.researchgate.net/publication/376950970\\_SECURITY\\_ANALYSIS\\_OF\\_THE\\_NATIONAL\\_MARITIME\\_TRANSPORTATION\\_SYSTEM\\_AS\\_PART\\_OF\\_THE\\_MARITIME\\_CRITICAL\\_INFRASTRUCTURES#fullTextFileContent](https://www.researchgate.net/publication/376950970_SECURITY_ANALYSIS_OF_THE_NATIONAL_MARITIME_TRANSPORTATION_SYSTEM_AS_PART_OF_THE_MARITIME_CRITICAL_INFRASTRUCTURES#fullTextFileContent) [Accessed: Feb. 06, 2024].
- [15] V. Stavev, "The Systems Approach: a Small Tactical Unit", Security Horizons, Volume III, No. 6, pp 151-157, September 2022. Available: UKLO, <https://fb.uklo.edu.mk/wp-content/uploads/sites/10/2022/10/TOM-1.2022-konecen-1.pdf#page=151> [Accessed: Jan 20, 2024], DOI: 10.20544/ICP.3.6.22. p15
- [16] Military security, Available: [https://connections.qj.org/system/files/13.3.04\\_szpyra.pdf](https://connections.qj.org/system/files/13.3.04_szpyra.pdf) . [Accessed: Nov. 3, 2023]

# *Model of management of processes and phenomena's in the military security system*

**Rumen Marinov**

*Security and Defense Faculty  
Vasil Levski National Military  
University*

Veliko Tarnovo, Republic of Bulgaria  
ramarinoff@gmail.com

**Abstract.** This paper presents theoretical analyzes and assessments of governance models in the military security system in the context of dynamically changing national security. The model for managing processes and phenomena in the system has been studied.

**Keywords:** *military security, processes, security policy*

## I INTRODUCTION

Considering national security as a complex public system with the force of imperative requires the perception of processes and phenomena in the military security system that make it unity, integrity, interconnectedness, and contradiction. The main processes of strategic security management directly correspond to different aspects of the environment of any nature, characterized by dynamism, unpredictability, and uncertainty [1].

The complex and complicated concept of military security „defines a problem with too broad a range that allows different interpretations depending on the interests of the participants themselves in the discussion [2].

Analysts' expectations that the information technology era will reduce the complexity and confusion of the battlefield are far from being met. Thus, in modern threat scenarios, the pursuit of technological superiority has proved to be an insufficient condition for success in network-centric wars. The human factor has once again been placed on the entire chain of command as an opportunity to deal with the growing amount of information and the need for timely decisions [3].”

## II MATERIALS AND METHODS

This research delves into an in-depth analysis of the challenges to national security in light of the evolving risks

and threats that have arisen in the current security landscape. The study aims to provide comprehensive insights into the implications of these changes and their potential impact on the security environment. It is crucial for us to prioritize the establishment and execution of a novel security and defense policy that is rooted in scientific principles. This policy should encompass all facets of military security and must be complemented by effective implementation strategies that ensure its success.

## III RESULTS AND DISCUSSION

In 2018, the external environment of security retained its complex and dynamic character, caused by changes in the equilibrium of forces in geopolitical, economic, and military terms. In the year, national interests and the fight for supremacy prevailed on a global and regional level. Variable international relations predetermined the main threats and risks for the national security and the interests of the Republic of Bulgaria. There have also been attempts to have a hybrid impact on a country, including action to influence in various aspects - political, economic, diplomatic, cultural, and propaganda. The unstable crisis processes in the Balkans, the Middle East and North Africa, Central and Southeast Asia are a major source of instability, political, economic, and asymmetric threats and risks for the country. The rapid development of technology for the production of weapons of mass destruction, as well as North Korea's aggressive foreign policy, continues to be a serious challenge to the international community.

Europe's tendency to be the desired destination for legal and illegal migration from North Africa, the Sahel, the Middle East, Central, and Southeast Asia is preserved. A Migration Agreement between the Turks and the EU was concluded in 2016, and despite its implementation, the potential threat to our country's security was maintained. The

*Print ISSN 1691-5402*

*Online ISSN 2256-070X*

<https://doi.org/10.17770/etr2024vol4.8188>

© 2024 Rumen Marinov. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

illegal crossing of the state border on the road to Europe continues to pose a threat to national security. There is a risk of penetration or transit of radicalized entities across the territory, as well as the involvement of organized crime groups in this traffic. Consequently, the challenges to the national security policy arising from the dynamics of changes in existing threats and risks in the new security environment require the formulation and implementation of a new science-based security and defense policy, military security, and strategies for their implementation.

The field of military security is vast and complex, encompassing a range of processes and phenomena that require careful examination and analysis. To ensure the safety and security of a nation, it is essential to identify and understand the sources of threats, as well as the defensive institutions that are specialized in managing those threats and mitigating the associated risks. Ultimately, military security is a critical domain that falls squarely within the purview of the state, demanding a high degree of competence, responsibility, and commitment.

#### IV TYPES OF MILITARY SECURITY SYSTEM CONTROLS

This means that intensive and in-depth analyzes of dynamics in changing the modern security environment, the needs and interests of civil society, security policy reform, and new security sector legislation, set up conditions for the conduct of Strategic Management. Because of this modern managers face the need to continually develop their skills [4].

Different researchers reveal separate and common states of military security. For example, in one of his analyzes, Nikolay Iliev directs himself to reveal the elements and factors influencing the planning process and the formation of the armed forces. The establishment of the respective troop organization includes activities on the scientific justification of the necessary organizational structure, machines, armaments, and training; equipment, personnel; setting up a training, training and military service system; establishment and operation of a management and military administration subsystem; establishment and operation of a mobilization subsystem; creation, maintenance, and development of a military command subsystem in the course of military and non-military actions in national and coalitions, etc. [5].

Given the current landscape of threats and risks, it is important to evaluate whether the system of security, particularly in the context of military security, is functioning effectively and in a state of equilibrium.

Human understanding of the world is constantly evolving despite the vast amount of knowledge we have. The discoveries made through new research often raise new

questions and unresolved issues, requiring new explanations and theories to be developed. In this sense, physics is in a continuous process of development and is still far from being able to explain all natural phenomena and processes [6]. The interplay between economic growth and sustainable development is a recurring theme, with discussions centering around the potential effects...[7].

The answer can be found in the 8<sup>th</sup>-grade physics textbook, which states that „Equilibrium is a state of a system, in which the equivalence of all external forces acting on each point of the system is zero. There are three types of balance in mechanics - steady, unsustainable, and indifferent. „When the force of gravity is balanced by the response force of the support, the kind of balance can be determined by the position of the center of gravity.

The answer may be in the Toricelles rule: If the center of gravity occupies the lowest position compared to all possible adjacent positions, then the balance is steady.

Here we find the place of physics that explores and describes physical objects and systems [8]. The task of managing theory is to transform the management style with the help of controlling influences to form a prescribed behavior.

When it comes to ensuring military security, the implementation of process and phenomenon management theory is crucial. However, this can only be achieved effectively by applying system management theory. In summary, properly managing processes and phenomena within the military security system requires a well-structured and systematic approach. To effectively manage military security systems, it is crucial to have a solid understanding of the various models of management objects, management objectives, and management algorithms. Additionally, it is important to clearly understand the basic methods involved in creating effective algorithms for managing these systems and the results that can be achieved. However, given the complexity and scope of this subject, When dealing with complex problems, it can often be quite difficult to comprehensively address and account for all of the pertinent issues and factors involved. Indeed, such situations frequently require a great deal of careful analysis, consideration, and thoughtfulness to arrive at an effective and well-rounded solution or approach.

According to the most popular management definitions, it is the organization and coordination of activities following certain policies to achieve clearly defined goals and a set of authority powers and decision-making responsibilities. As a discipline and practice, management is the process of planning, forecasting, organizing, managing, coordinating, controlling, and regulating all the elements and resources of the organization [9].

In all types of management, a level of uncertainty exists. In each situation, all or most of the factors creating uncertainty act to varying degrees. For this reason, each decision made at a given time will lead to a different result [10]. The type of management chosen for the military security system has to provide reliable and robust decision-making on all levels.

The control theory works with three types of controls: parameters are constant functions of time, parameters are variable functions of time and parameters are a combination of the first two. They use state variables that control variable and output (observable) variables.

**In the first type of control** – In a system, the control or control parameters are functions that remain constant over time. These parameters play a critical role in optimization tasks as they help in finding the optimal value of a control parameter that can provide a minimum or maximum value of a set function of the system. However, it is important to note that setting a definite value in value over time may not always produce the desired effect as it could affect the system's modes of operation. Hence, careful consideration and analysis of the control parameters are crucial for ensuring optimal system performance.

**In the second type of control** – The concept of control parameters as variable time functions is integral to the study of the behavior and properties of systems and materials in uncertain or hesitant actions, where the effects are harmonious. One key aspect of such systems is their ability to be managed and controlled, which is a function of time. Depending on whether the control influence depends solely on time or other factors as well, the mode of control can be either programmatically or interference/open-loop control. This nuanced understanding of control theory is essential for designing and implementing effective control systems in a wide range of domains, from engineering to biology. Programming may depend on parameters as well as on the initial conditions of the control object:

$$u(t)=U(t,x_0) \quad (1)$$

The third type of management, parameter management is a combination of the first two in the form of  $u(t) = const$  or  $u = u(t)$  defining the simplest forms of management. Even greater capability is the controlling influence that is used to calculate the results of  $u(t)$  a site's measurement or outputs. Such control is recorded in a status feedback form:

$$u(t)=U(x(t)) \quad (2)$$

or at exit:

$$u(t)=U(y(t)) \quad (3)$$

where “x” and “y” are the vectors of the state and outputs of the system.

Feedback management has significantly more capabilities and allows the system properties to be substantially changed. However, this may sometimes result in negative results from such methods, such as influencing the measurement, changing the system of equations describing the system, and therefore testing another system. In physical tasks, the impact is subject to strict limitations - requirements for small values of management [11] [12].

The study suggests that every impact experiment on the military security system brings about some changes, even without feedback. Even a simple observation of the system could distort its natural course, which follows the principles of quantum mechanics. However, despite this, conducting experiments is still a useful means of studying the system.

In the military security system, it is assumed that phenomena and measurement processes do not impact the dynamics of the site and can be disregarded. However, this assumption does not hold for microsystems and objects, as these may be affected by even the smallest changes in their environment or measurement processes. Therefore, it is essential to consider these factors when dealing with microsystems and objects to ensure their proper functioning and security.

Both in physics and in the military security system, it is manageable if:

- it has a separate parameter and/or parameters called input or control, the change of which leads to changes in some behavioral characteristics of the system called outputs;
- it has a separate parameter and/or parameters called input or control, the change of which leads to changes in some behavioral characteristics of the system called outputs;[13]
- the area of the behavior of the system, the parameter at the control capability limits, which corresponds to the desired modes of operation of the system.

#### V MODELS OF MILITARY SECURITY MANAGEMENT OBJECTS

In the realm of physics, a wide range of phenomena can be described using differential equations. However, some of these equations are private and cannot be easily studied. For this particular investigation, only ordinary differential equations will be used. These equations are known for their simplicity and ease of analysis, making them a popular choice for many scientific studies. The patterns of

management objects described with them in the state space are represented by:

$$\dot{x}=F(x,u) \quad (4)$$

where  $x=x(t)$  is the n-meter vector of component state variables  $x_1, x_2, \dots, x_n$ , and the components of the control effects are  $u_1, u_2, \dots, u_m$  also  $u = u(t)$  is a m-vector vector at the inputs of the control variables. The system of ordinary differential equations is:

$$\frac{dx_i}{dt} = F_i(x_1, x_2, \dots, x_n, u_1, u_2, \dots, u_m), \quad i=1, 2, \dots, n \quad (5)$$

$\frac{dx_i}{dt}$

$F(x,u)$  must satisfy the conditions for the existence and uniqueness of the decision with initial conditions  $x(0)$ .

When the input variables are dimensions like forces, moments, intensity, etc., objects are coordinated. If the input variables represent a change in the system parameter values, the objects are parametric control. For example,  $u(t)=p-p_0$ , where  $p_0$  is the initial value of the parameter. Input variables can also be represented here by the relative change in system parameter values. Then  $u(t)=p/p_0$  is a dimensionless dimension.

The Model of Controls in the Military Security System is convenient for describing the management of the dynamics of objects with discrete models.

$$x_{k+1} = \bar{F}_k(x_k, u_k), \quad y_k = h(x_k) \quad (6)$$

where  $x_k, u_k, y_k$ , state vectors, inputs and outputs of the process step  $k=0, 1, 2, \dots$ , the discrete model is set with a set of  $\bar{F}_k$ . Switching to a discrete model is convenient, even for continuous processes, as the measurement takes place at discrete times. Then:

$$x_k = x(t_k), \quad u_k = u(t_k), \quad y_k = y(t_k) \quad (7)$$

We can conclude that the model of military security consists of common instruments and commitment to security, freedom, and the inviolability of human life, which leads to their mutual reinforcement.

## VI CONCLUSIONS

It is necessary to counteract the causes of insecurity, to improve prevention, and to anticipate action [14]. To ensure the safety and protection of citizens, it is important to involve all relevant sectors, including the political, economic, and social sectors, as appropriate. Additionally, there should be a greater emphasis on the interdependence between internal and external security measures. By working together across sectors and focusing on interdependence, we can create a

more comprehensive and effective approach to safeguarding individuals and communities.

As a means to ensure the military security of nations, it is feasible to establish stronger partnerships with existing international security organizations. It is important to note that while achieving some short-term goals without actively engaging with various organizations may be possible, it is imperative to do so in the long term for a country to achieve strategic success. Building and maintaining relationships with these organizations can provide valuable insights and resources that can lead to sustainable growth and success. Therefore, countries should prioritize actively engaging with relevant organizations to ensure long-term success.

## ACKNOWLEDGMENTS

This paper 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] 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, ISBN: 978-172813467-3, DOI: 10.1109/CREBUS.2019.8840098, pp. 156-160
- [2] S. Stoykov, Science and knowledge in the management of the security system, Monography, V.T. 2018, ISBN 978-954-753-276-2, p. 114, pp.14
- [3] E. Petrova, Basics of Management, Publishing complex of Vasil Levski NMU, V. Turnovo, 2013, ISBN 978-954-753-121-5, pp. 21-27
- [4] V. E. Dimitrova, The impact of coaching on the emotional intelligence of managers in the organization, 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, pp. 276-280
- [5] N. T. 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
- [6] N. Iliev, Terms and Requirements in Planning and Formation of Forces, Union of Scientists in Bulgaria – Veliko Turnovo, 2011. // Union of Scientists in Bulgaria, May readings „Days of Science 2011”, Veliko Turnovo, 27 May 2011, volume 2, ISSN 1314-2283), pp. 509-516
- [7] N. T. Dolchinkov, Optimizing energy efficiency in the conditions of a global energy crisis, Release Date: September, 2023] Pages: 408, DOI: 10.4018/979-8-3693-0400-6, ISBN13: 9798369304006], EISBN13: 9798369304013, pp. 1-9
- [8] N. T. Dolchinkov, and M. Pdvlov, Influence of meteorological elements in accidents in enterprises with radioactive elements or dangerous chemical substances in Bulgaria, 14th International Scientific and Practical Conference Environment. Technology. Resources. Vide. Tehnologija. Resursi, 2023, ISSN 1691-5402, 1, pp. 49-54
- [9] V. Statev, “Training for Uncertainty”, HORIZONS, Year XIV, Volume 29, pp. 271-276, December 2021. Available: UKLO, <https://uklo.edu.mk/wp-content/uploads/2021/12/23..pdf> [Accessed January 18, 2024], DOI 10.20544/HORIZONS.A.29.2.21. pp.23-28



- [10] P. Marinov, Contemporary Challenges to Security System Management and Counter Terrorism, East-West, 2016, Sofia, 2017, ISBN 978-619--01-0027-0, pp. 71
- [11] E. Petrova, "Influence of Military Organizational Culture on Individual Performance of The Learners of the Example of The Vasil Levski National Military University, Bulgaria," 2019 International Conference on Creative Business for Smart and Sustainable Growth (CREBUS), Sandanski, Bulgaria, 2019, DOI: 10.1109/CREBUS.2019.8840105, pp. 1-4
- [12] St.Pancev, Chaos Theory, Sofia, Ac. edition. profesor Marin Drinov, 2001
- [13] L. Lazarov, General terms and conditions for the radio connection jamming, National conference on High Technology for Sustainable development HiTech 2018, Institute of Institute of Electrical and Electronics Engineers Inc. ISBN: 978-153867039-2 DOI:10.1109/HiTech.2018.8566645, pp 131-133
- [14] P. Marinov, Contemporary Challenges to Security System Management and Counter Terrorism, East –West, 2016, Sofia, 2017, ISBN 978-619--01-0027-0, pp. 34

# *Use of Artillery Fire Support Assets in the Attrition Approach in the Russia-Ukraine Conflict*

**Dilyan Markov**

*Rakovski National Defence College*

Sofia, Bulgaria

dilyanmarkov@abv.bg

**Abstract.** The armed conflict between Russia and Ukraine since February 24, 2022 does not appear to have a clear end, but to trace the possible paths of development, a better understanding of the strategy of waging war by the armed forces of both countries is needed. More detail on the attrition approach would facilitate realistic estimates of the duration of military conflict and the likely costs of artillery systems and munitions used in it.

The causes and aspects of the implementation of exhaustion and its relationship with the amount of artillery ammunition used, develop the direct dependence on the increased need for their use. The influence of post-Soviet fire support assets on the different combat use procedures applied by the Ukrainian forces and the provision of Western-style weapons of varying types and quantities indicate the reasons for the implementation of the attrition strategies.

The use of the artillery systems according to the stock method and the available amount of ammunition for them leads to the impossibility of applying their capabilities in a full profile on the battlefield to achieve the goals set by the political demands.

**Keywords:** *attrition approach, artillery, fire support, conflict between Russia and Ukraine.*

## I. INTRODUCTION

Historically, wars between states have varied in duration, influencing the outcome of each of them, regardless of the plans of the opposing sides. In this aspect of the statement is also what was indicated by the Prussian general and military theorist Carl von Clausewitz, who observed that armed conflicts are full of unpredictability, as "things happen differently from what we expected [1]".

Regardless of advances in technology, the factors of space and time remain valid today for the conduct of operations by the armed forces. For the advancing troops, the goal is to gain space as quickly as possible while the defenders try to maintain control of the territory and delay or deny further action to the attacking enemy. Therefore, any time gained is to the advantage of the defender, because the combat power of the attacker is likely to decrease over time. For the smaller country, ceding space may not lead to any advantage, but any space gained will equal time gained.

For any conflict, the type and manner of use of the armed forces and, in particular, the means of artillery fire support are relevant to the above factors. Applying their effect in conjunction with tactics, techniques and procedures affects the duration of each operation. Their application is related to the possibility of use in any weather conditions and in a prolonged time interval in a direct combination with the approaches of the operational and tactical actions of the maneuver formations, bordering on endurance and exhaustion, as a means of achieving the goals.

## II. MATERIALS AND METHODS

Various literary sources related to the initial analysis of the war in Ukraine point to the development of the situation leading to a war of attrition. The effects of which and the role of field artillery in it are the subject of research, through the separation of different triggers, consistently argued by the author, who, from the point of view of an artillery specialist with practical experience with post-Soviet guns, characteristic of the conflict and theoretically examining the problems of this type means of shooting, shows the transformation of artillery in different directions.

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8208>

© 2024 Dilyan Markov. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

The report uses a variety of scientific methods to analyze the role, functions and tasks of artillery in the conflict - scientific analysis and synthesis, argumentative analysis, analysis of individual statements. The influence of the number of artillery rounds fired, the performance of field artillery tasks, compared to the theory of fire support planning, but not least on the endurance of artillery systems in the conflict, has been studied consistently.

### III. RESULTS AND DISCUSSION

To indicate the changes in the use of artillery in the conflict, the analysis of the fighting will be dated February 24, 2022, when Russia launched a full-scale attempt to take the capital of Ukraine by invading and conquering the entire country. These actions resembled the Soviet occupation of Czechoslovakia in August 1968, as well as the takeover of Afghanistan on 27 December 1979 [2].

This so-called "special military operation" [3], [4], [5] according to some researchers failed to achieve its political goal of replacing the incumbent Ukrainian government, which the Kremlin expected to fall within four days [5], [6], but according to others, "Russia's aim was not to conquer territory [4]".

Ukraine's military strategy was initially based on defense in depth or, in some cases, mobile defense, which then shifted to the offensive. In this aspect, offensive efforts proved partially successful in the fall of 2022, as the conditions were determined by the structural shortage of personnel of the Russian forces. The impact of attrition resulted in significant combat losses, refusal to enter combat, and low morale [7]. The war in Ukraine has become a war of attrition, a major approach for both Ukraine and Russia at the tactical level, with neither side having gained much territory from Ukraine's successful offensives (defined by Jacques Baud [8] as counterattacks) in late 2022 although the number of victims has increased. In this context, John J. Mearsheimer concludes that "... the cost of an attrition strategy is always high" and "... success is relatively uncertain." from their stronger opponents [9].

More broadly, attrition is a key element of Ukraine's shift in strategy. This finding should not be surprising since its army has artillery units similar in structure to Russian forces. Neither army looks like it did at the beginning of the war, each of which has become a heterogeneous force made up of mobilized personnel, auxiliaries, foreign fighters and, in the case of Russia, mercenaries (including ex-prisoners in the private military Wagner Company) [10]. Also, even emphasized at the beginning of the conflict "continuous successes of the defense complex and the armed forces of the country in terms of putting into operation novelties in armaments and equipment in the troops, which completely changes the tactics and operational art of the Russian army" [11] have reduced to the current state of attrition strategy.

The effects of exhaustion are evident on both sides. The Ukrainian military appears incapable of executing a large-scale combined maneuver, and a key question is how quickly the Ukrainian armed forces can restore their

capability to conduct sustained operations against Russian forces. On the other hand, "Russia operates within a Clausewitzian mindset in which operational successes are used for strategic purposes. Therefore, operational strategy plays an essential role in defining what counts as a victory" [4].

In the midst of the analyzed conflict and over time, as well as the way the operation was conducted, it showed that the possibility of victory of the armed forces of Ukraine decreases significantly, due to the fact that Russia is becoming stronger in every element of power. In the context of this statement is the statement of General Christopher Cavoli, Supreme Allied Commander Europe (SACEUR) and Commander, U.S. European Command, to a US Congressional committee that "Russia's air, naval, space, digital and strategic capabilities have not suffered significant degradation during this war [4]".

Characteristic of the last months of the military conflict is that the contact line stretches over 1,000 km. [12] and affects tactics, with both sides having distributed their manpower and firepower along the entire front. Although the nature of the fighting may yet change, most signs point to a protracted war of attrition in eastern and southern Ukraine [13]. In recent months, attacks and attempted breakthroughs have occurred only in isolated parts of the battlefield. This enables the troops to entrench and systematically expand their own defensive positions, and trenches, mined areas, destroyed roads and bridges, and support from their own artillery make it almost impossible to overcome the enemy's defensive lines [12].

A claim that field artillery could play an important role in hostilities between Ukraine and Russia was published by Sam Cranny-Evans at The Royal United Services Institute just ten days before the escalation of the conflict. It analyzes the Russian way of waging war, using tactical and operational systems for indirect fire support against enemy forces, contrasting Ukraine's ability to conduct counter-battery combat as a decisive influence on the outcome of the conflict between the two countries [14].

This statement is confirmed by the way the war was conducted, where both sides made significant use of missile troops and artillery, which became the main means of fire support for ground forces due to limitations in the use of aviation [15], [16]. An important fact is that at the beginning of the war, Ukraine had over 1,000 122 mm, 152 mm and 203 mm guns and 1,680 rocket launchers, 122, 220 and 300 mm calibers, more than Great Britain, France, Italy, Spain and Poland combined, placing it as the second European artillery power after Russia [16], [17].

In the approach of attrition applied by both sides, the use of means of artillery support are the subject of research by a number of experts [2, 10, 12]. Analyzing the conflict, Franz-Stefan Gady and Michael Kofman point out that "Ukraine's preferred mode of warfare centers on the use of artillery fire in the interest of decisive and debilitating effects on the enemy combined with maneuver [10]." An example of this type of action are large conventional wars involving attrition, maneuver

and recovery. Winning a war of attrition requires a willingness to incur significant casualties and significant losses of armaments, equipment and materiel.

The war in Ukraine was characterized by extensive use of engineering equipment, various forms of offensive actions of infantry formations characteristic of mass armies, significant use of fire support and heavy losses in personnel, weapons and equipment on both sides.

During the hostilities, Ukrainian forces sought to degrade the physical, mental and morale of Russian forces by targeting critical support systems such as command and control posts and logistics storage facilities. These actions were achieved primarily through attrition tactics combined with increased artillery fire as a result of significant military support from various types of artillery systems. Such, that affected their combat use, because their availability, as well as the ammunition provided for them, varied daily.

Analysis the indicate relatively independent use of artillery systems, which is not characteristic of their combat use procedures. This leads to inefficiencies in the offensive actions of the maneuver forces against a prepared enemy defense, often with a high density of positions, because a number of literary sources, both from the post-Soviet era [18] and current ones [19, 20] point out, that the characteristic features of modern combined-arms combat include simultaneous or sequential powerful fire action along the entire depth and the entire front.

The extent of the use of the means of fire support is also evidenced by the analyses of the ammunition used for the field artillery, launchers and anti-tank means. Despite the presence of many inaccuracies and large tolerances in the data in the following lines, the hypothesis of the massive use of artillery in this conflict is confirmed.

It is an indisputable fact that at the beginning of the war, Russia had vast stockpiles of 122, 152 and 203 mm shells, as well as 122, 220 and 300 mm rocket ammunition [16] which included post-Soviet quantities, as the storage methods used (also used in the other countries of the former Warsaw Pact) allows their use in the conflict, even with increased risks of accidents.

Some reports indicate that up to 20,000-40,000 shells and rockets are fired per day by Russia [14] while the European Commission figures that in early 2023, Russia was firing between 40,000 and 50,000 artillery shells each day, and the Ukrainian fire support forces use between 5,000 and 6,000 shells to perform fire missions [21]. Expert estimates by the Estonian government point to altered figures of between 20,000 and 60,000 Russian shells and 2,000 to 7,000 Ukrainian artillery shells per day on average [22].

Various estimates of the Russian artillery fire are also given by a number of American and Ukrainian officials, the first of which indicates that the rate has dropped from 20,000 to about 5,000 per day on average, while according to Ukraine the drop is from 60,000 to 20,000 per day [23]. Estimates from another source [24] indicate an average of 4,000-7,000 artillery shells per day throughout the conflict for Ukrainian forces by the

end of 2022, while Russian rates ranged from double to quadruple the Ukrainian rate.

Analyzing that the line of contact has been almost unchanged for quite some time, which can be pointed out as a crisis and an element of exhaustion, the artillery has become the most important factor in holding this parity. Artillery requirement data is an important part of planning any operation involving fire support systems, being the key to success in solving war objectives.

The tasks of field artillery do not differ from the doctrinal concepts of both the armed forces of the Russian Federation and Ukraine [16]. This is a fact for both countries, as part of a former union (Warsaw Pact), for Russia to a greater extent, for Ukraine, as a legacy, insurmountable even after training by Western specialists. In this context, analyzing the theory of fire support planning [20], it can be determined that the targets of the post-Soviet era were determined three times more than the capabilities of the guns, as a large part of them were unobservable. Perhaps this is precisely the seed of the problem tied to the way ammunition is spent.

Both sides most likely used at the beginning of the conflict the rules for hitting single and group targets inherent in the theory of ground artillery fire. According to them, the number of munitions to hit non-observable targets is four times higher than that of visible ones. Characteristic of this type of fire attacks are the different procedures determining the method of firing at the targets. The number of batteries (platoons, guns) performing the firing task depends on the nature, importance and dimensions of the target, firing tasks, firing distance and mode of fire, as well as on the available time and conditions for performing the firing task. In such a case, the mass use of fire support (fire massing) leads to the simultaneous or sequential concentration of the most important groups and objects of the enemy or to the distribution of fire to simultaneously strike several groups or objects, leading to the indicated large amounts of ammunition expenditure for day or month.

One element of the theoretical formulation mentioned in the previous paragraph is the mode of fire of the artillery systems, the indicators of which are limited mainly by the capabilities of the cannon calculations and the material part. As it refers to the guns during firing of arbitrary duration, it is necessary to distribute the shots approximately evenly throughout the entire time of conducting fire, while after an interruption (interruptions) lasting less than 20 min, it is determined by the total time of firing, including the interruption(s). However, cannon barrels have a set lifespan that varies from manufacturer to manufacturer. In his article, Patrick Hinton [25] states that howitzer barrels have a life of between 1500-2500 rounds before needing to be replaced. I cannot agree with him, especially for the post-Soviet types, for which it is stated that at 4000 rounds the wear of the charging chamber has a variable sign, affecting the initial velocity of the projectiles (in rifled systems). However, pressing questions about reparability remain because nearly 1/3 of the artillery inventory is out

of service for maintenance and repair at any given time [25].

The aspects mentioned here have certainly determined the change in tactics and the concept of the combat use of fire support assets. The decrease in ammunition consumption is certainly influenced by the method of firing on the targets and reduced supplies, both to Russia and Ukraine. Various data indicate the use of single systems, somewhat up to two, and in extreme cases in a platoon, caused by the need to protect the forces on the one hand and a shortage of gun systems and ammunition for them on the other.

The shortage of ammunition is clearly discernible. Data on supply reduction are conflicting, but various studies on the matter [16] point to the limitations imposed.

For Ukraine, there is a serious shortage of artillery ammunition, both for post-Soviet equipment and for provided Western samples. For the first type, even if they were provided with those from the countries of the former Eastern bloc, the increased amount produced in Ukraine and other countries could not provide the needs of the artillery, and over time, however, their stocks were exhausted. Ukrainian artillery, along with the supply of Western guns, became entirely dependent on the supply of Western ammunition, mainly 155 mm cannon ammunition and 227 mm rocket ammunition. At the beginning of 2024, it turned out that the situation was becoming critical, and the Minister of Defense Rustem Umerov described the situation as "shell hunger [26]".

The European Union has pledged to deliver one million shells by March 2024, but it appears that the amount will be less than half that by the end of the year.

The United States has already provided Ukraine with over 800,000 155 mm shells [27], while Ukraine is asking for 250,000 per month [28]. Although the Pentagon believes it can expand production of 155 mm ammunition, the war has nevertheless consumed at least six years of 155 mm production [29].

For Russia, stocks of ammunition were starting to run out, and production rates were not enough, which forced the country to increase their production by about 50 times, but in addition, shells were purchased from North Korea, Egypt and Iran [16], [26].

Another direction in the current analysis is the type of artillery systems. It was pointed to the availability of Ukrainian artillery at the beginning of the conflict, but the depletion of ammunition reserves for them, combined with the approach of deterrence through the supply of arms, equipment and ammunition by the countries supporting the country, changed the nature of the artillery potential. In mid-2023, Ukraine had 14 different modifications of Western-made artillery systems in its ground forces [25]. Their main caliber is 155 mm according to the NATO standard, but not every artillery installation can use every projectile of this caliber. Guns and ammunition must be compatible. The difference in ammunition creates many opportunities to supply unsuitable ammunition because some NATO standard 155 mm guns are more compatible with some shells than others.

At the heart of the rift is the question in the ongoing war at a key geopolitical location [30]: how long can the two powers sustain the supply of said ammunition and the maintenance of artillery systems? With the answer, the need to change the tactics of using field artillery in a conflict of attrition, where fire support is one of the significant factors for its implementation, can be unambiguously determined.

#### IV. CONCLUSIONS

The continuation of hostilities between Russia and Ukraine with the use of attrition tactics by both sides inherently affects the development of the art of war. Artillery formations, as means of implementing fire support for the ground forces, are undergoing transformation in various directions.

The first of these is the massing of artillery fire as a means of achieving enemy attrition with heavy expenditure of artillery ammunition of all types and calibers, leading to wear on gun barrels and leading to ammunition supply challenges.

The second is a change in combat use depending on the available artillery systems, their type, available ammunition stocks, and the need for battlefield survivability.

The third is the resurgence of the role of artillery in armed conflict, a fact that is little dismissed but practically confirmed in the circle of military art over the years and proves that the joint action of the various components in the domains of the operational environment is a factor of application according to availability and necessity.

#### REFERENCES

- [1] C. v. Clausewitz, *On War*, Book Three, New York: Penguin Books, 1668.
- [2] F. Heisbourg, "How to End a War: Some Historical Lessons for Ukraine," *Survival, Global Politics and Strategy*, vol. 65, no. 4, Jul. 7, 2023.
- [3] Ya. Streletskiy, "Spetsialnaya voennaya operatsiya Rossii na Ukraine: Aksiologicheskii aspekt," *Gumanitarnye, sotsialno-ekonomicheskie i obshtstvennye nauki.*, vol. 6, June 2023. [Я. Стрелецкий, "Специальная военная операция России на Украине: Aksiologicheskii aspekt," *Гуманитарные, социально-экономические и общественные науки.*, vol. 6, June 2023.]
- [4] J. Baud, "The Russian Art of War: How the West Led Ukraine to Defeat," Jan. 1, 2024. [Online]. Available: <https://www.thepostil.com/the-russian-art-of-war-how-the-west-led-ukraine-to-defeat/> [Accessed Feb. 7, 2024].
- [5] D. Minic, "What Does the Russian Army Think About its War in Ukraine? Criticisms, Recommendations, Adaptations," *IFRI*, vol. 44, Sept. 21, 2023.
- [6] A. Coleman, "Ukraine Crisis: Russian News Agency Deletes Victory Editorial," Feb. 28, 2022. [Online]. Available: <https://www.bbc.com/news/technology-60562240> . [Accessed Dec. 16, 2023].
- [7] R. Dalsjö, M. Jonsson and J. Norberg, "A Brutal Examination: Russian Military Capability in Light of the Ukraine War," *Survival, Global Politics and Strategy*, vol. 64, no. 3, p. 7–28, June 2022.
- [8] J. Baud, "Our Latest Interview with Jacques Baud," Sept. 1, 2022. [Online]. Available: <https://www.thepostil.com/our-latest-interview-with-jacques-baud/> . [Accessed Dec. 21, 2023].

- [9] J. Mearsheimer, *Conventional Deterrence*, NY, 1985.
- [10] F. Gady and M. Kofman, "Ukraine's Strategy of Attrition, Survival," *Survival, Global Politics and Strategy*, vol. 65, no. 2, pp. 7-22, Mar. 28, 2023.
- [11] V. Vasilev, "Realizirani ot Rusia hibridni zaplahi v sektora na sigurnostta i otbranata na Republika Bulgaria", *Veliko Tarnovo*, p. 215-220, 2023. ISSN 2367-7473. [ В. Василев, "Реализирани от Русия хибридни заплахи в сектора на сигурността и отбраната на Република България" стр. 215-220, 2023. ISSN 2367-7473.]
- [12] T. Lachan, "Okopna voyna: novata deystvitelnost na fronta v Ukrayna," [Т. Лачан, "Окопна война: новата действителност на фронта в Украйна,"] Nov. 5, 2023. [Online]. Available: <https://www.dw.com/bg/okopna-voyna-novata-dejstvitelnost-na-fronta-v-ukrajna/a-67308708> [Accessed Feb. 1, 2024].
- [13] S. Jones, R. McCabe and A. Palmer, "Ukrainian Innovation in a War of Attrition," February 2023. [Online]. Available: <https://www.csis.org/analysis/ukrainian-innovation-war-attrition> [Accessed Jan. 10, 2024].
- [14] S. Cranny-Evans, "The Role of Artillery in a War Between Russia and Ukraine.," *The Royal United Services Institute*, Feb. 14, 2022.
- [15] A. Jash, "A Litmus Test for the Future," Jan. 25, 2024. [Online]. Available: [https://www.researchgate.net/publication/377691343\\_A\\_Litmus\\_Test\\_for\\_the\\_Future\\_of\\_Artillery](https://www.researchgate.net/publication/377691343_A_Litmus_Test_for_the_Future_of_Artillery) [Accessed Feb. 8, 2024].
- [16] 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.
- [17] S. Ganjiyev , S. Usmonov and A. Karimov, "Use of artillery in modern war (A brief analysis of the ukrainian conflict," *Galaxy International Interdisciplinary Research journal (GIIRJ)*, vol. 11, no. 3, March 2023.
- [18] *Taktika na artileriyata*, Sofia: Darzhavno voenno izdatelstvo, 1971. [Тактика на артилерията, София: Държавно военно издателство, 1971.]
- [19] *Tashkov i kolektiv, Taktika na mehaniziranite i tankovi formirovaniya*, Sofia, 2023. [Ташков и колектив, Тактика на механизираниите и танкови формирования, София, 2023.]
- [20] R. Chalakov, "Vliyanie na metoda za planirane na ognevata poddrzhka v operatsiite," *Sbornik dokladi ot mezhdunarodna nauchna konferentsia, Faculty of Artillery, Air Defense and Communication and Information Systems* pp. 206-212 2020 [Р. Чалъков, "Влияние на метода за планиране на огневата поддръжка в операциите," Сборник доклади от международна научна конференция, pp. 206-212, 2020. ISSN 2367-7902]
- [21] J. Rankin, "EU seals deal to supply Ukraine with a million rounds of shells," *The Guardian*, Mar. 20, 2023. [Online]. Available: <https://www.theguardian.com/world/2023/mar/20/eu-deal-supply-ukraine-ammunition> [Accessed Feb. 8, 2024].
- [22] M. R. Sahuquillo, "Ukraine Outgunnes 10 to 1 in massive artillery battle with Russia," 2023.
- [23] N. Bertrand, O. Liebermann and A. Marquardt, "Russian Artillery Fire Down Nearly 75%, US Officials Say, in Latest Sign of Struggles for Moscow," *CNN*, 10 January 2023.
- [24] C. Kube, "Russia and Ukraine Are Firing 24,000 or More Artillery Rounds a Day," *NBC News*, Nov. 10, 2022.
- [25] P. Hinton, "Lean on the Barrage: The Role of Artillery in Ukraine's Counteroffensive," *Royal United Services Institute*, Jul. 12, 2023.
- [26] V. Melkozerova and E. Hartog, "Ukraine's army is suffering artillery 'shell hunger'," *Politico*, Feb. 1, 2024.
- [27] M. Peck, "The US has given Ukraine nearly 1 million 155 mm artillery shells. Now it's looking for US companies to build more of them.," *Business Insider*, Sept. 14, 2022.
- [28] A. Bounds, "Ukraine asks EU for 250,000 artillery shells a month," *The Financial Times*, Mar. 3, 2023.
- [29] M. Cancian, "Rebuilding U.S. Inventories: Six Critical Systems," *Center for Strategic and International Studies (CSIS)*, Jan. 9, 2023.
- [30] T. Dimitrov, "Aspects in usage of unmanned surface vehicle in Ukrainian war", *Black Sea Security, Nikola Vaptsarov Naval Academy*, Varna, 2023.

# *Legal framework of the EU policy in the field of defence space technology*

**Tsveta Veselinova Monova**  
G.S.Rakovski National  
Defence College  
Sofia, Bulgaria  
ts\_monova@abv.bg

**Abstract.** The defence policy of the European Union is a reference point for development of legislation at supranational level that sets new dimensions for European integration. Maintaining a high-tech defence industrial base is among the key objectives that the Union sets itself in its security and defence policy. In this sense, a European defence policy focuses on cooperation between states to build, develop and upgrade the entire spectrum of land, air, sea and space defence capabilities. "Space is a strategic benefit essential to Europe's independence, security and prosperity." Space as a distinct operational area is of essential importance for the EU defence. The policies of the Union are aimed both at ensuring independent and autonomous access to outer space and development of various types of defence technologies. That will best enable rapid situational awareness, rapid decision-making and efficient operations. The space defence technology infrastructure established by the EU should meet the security needs of the Union. Based on this, the EU legal framework on space as a separate area of security and defence reveals different types of supranational legal instruments. They regulate specific military and political issues regarding space defence and technology development.

**Keywords:** *defence, European Union, legal framework, space technologies*

## I. INTRODUCTION

The military defence policy of the European Union is a reference point for the deployment of the legislative process at the supranational level in a direction that sets new dimensions of the European integration. On the international level, the main merit for its development is played by supranational legal and regulatory instruments of different types and degrees, which were adopted under the influence of various factors that directly threaten the European security environment, its citizens, such as the growing strong strategic competition between states and their ambition of military-political hegemony, the wide and varied by type spectrum of complex and unpredictable security threats, the direct attacks against the established European security order, etc.

"Space is a strategic asset central to Europe's independence, security and prosperity." [12] The growing on the international level competition to master the space sector is predetermining the political attitudes of the European Union regarding the same, turning it into a factor of strategic/key importance. Ensuring independent access to outer space and the development of various space technologies will lead to an increase in the defence capabilities of the Union in the rapid decision-making, the effective conduct of operations and providing the best opportunity for a quick and adequate assessment of the situation.

The space defence technology infrastructure established by the EU should meet the security-related needs of the Union. The Union's space industry is already one of the most competitive in the world. However, the emergence of new participants and the development of new technologies are fundamentally changing the traditional models in the field of industry. The remaining of the Union as a leading participant on the international political scene with wide freedom of action in the field of outer space is bound to promotion of scientific and technical progress and support in the competitiveness and innovation capacity of enterprises of the space sector within the Union, in particular of small and medium-sized enterprises (SMEs), start-ups and innovative enterprises. In many cases, the equipment, components and instruments used in the space sector, as well as space data and services, are dual-use. However, the Union's security and defence policy is defined within the framework of the common foreign and security policy in accordance with Title V of the Treaty on European Union (TEU).

## II. MATERIALS AND METHODS

In an attempt to analyze the special place occupied by outer space as a separate field and the related space defence technology industry established by a common regulatory legal framework of EU security and defence policy, it should be noted that the latter is currently deeply fragmented. The main reason for this is the fact that the

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8223>

© 2024 Tsveta Veselinova Monova. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

material field of application, which regulates these issues, cannot provide the European integration system with a universal and explicit legal regulation in this direction. In this sense, this systemic fragmentation, dating back to the early period of the union's emergence, leads to the formation of a legal mosaic of separate regulations scattered in the various legal sources of the common law of the union and dealing fragmentarily with separate issues of the integration military policy. This, in turn, causes a process of uneven regulatory and institutional development of the EU and creates practical difficulties in the implementation of the relevant supranational provisions.

Under the influence of the above-mentioned processes, the regulatory system of the European defence industry is highly fragmented and, in particular, the space defence industry. Outer space as a separate sector, characterized by its specificities and a particular trajectory of scientific research of a legal dimension, in so far as the latter obeys both the primary law of the EU, established by the provisions of the founding treaties of the EU, and other acts that have been adopted specifically for the purpose of regulating the legal matter.

Already at the very beginning of the preamble of the **Treaty on the Functioning of the European Union (TFEU) [14]** it is expressly proclaimed that one of the leading objectives around which the legal successor of the European Community is concentrated/consolidated is related to the unification of the states of this union from the idea of implementing a common and unified foreign and security policy, and in particular towards gradually taking successive steps towards the "formation of a common/uniform defence policy"[14], which could lead to joint/collective defence in accordance with the provisions of Art. 42 "[14], of the TFEU and through it in this way to achieve the strengthening of the European identity and its independence in order to promote peace, security of progress in Europe and in the world. This concept of the general collective defence of the parties, laid down by the above-mentioned fundamental in kind international treaty, is not new, in as much as the same is placed, subordinated and incorporates in itself the intention of the founders of the Charter of the United Nations, for individual or collective self-defence in hypotheses of carried out armed attack against a member of the Organization, as well as taking the necessary measures to maintain the international peace and security established worldwide. The envisaged package of measures related to taking immediate and specific actions in the event of an attack was created/exists by virtue of the special text established/ implemented by the rule of Art. 51[15].

In parallel with this, the following legal provisions from the TFEU are of particular legal ~~weight~~ importance in relation to the defence and security sector and in particular in the field of outer space of the EU, namely Art. 173 (ex Article 157 TEC) and those from title XIX of the TFEU - dedicated specifically to "Scientific research, technological development and outer space"[14]. In this sense, while the rule of Article 173"[14], of the TFEU aims to establish basic starting points related to guaranteeing the creation of more favourable conditions for the development of European industry and, more specifically, conditions related to "foster better

exploitation of the industrial potential of policies of innovation, research and technological development"[14], then this idea further finds confirmation and deployment in Title XIX of the TFEU by means of the foreseen multiannual framework programme of the EU in favour of scientific and technical progress and industrial competitiveness.

The main political positions that form the union in this programme are aimed at creating a stable European scientific and research space at the supranational level, including various types of cooperation and coordination initiatives between countries, as well as investing in various scientific and research activities. According to Art. 189 [14], of the TFEU is envisaged the development of a specialized legal act in the field of outer space, namely a European space policy.

At the same time, if an attempt should be made for a more in-depth study of the process of strengthening the EU's political interest in outer space and determining its starting point, it can be established that this process began towards the end of the 90s of the XX century. In the 1960s of the last century, the cooperation of the first structures of the member states led to the establishment of the first European intergovernmental organization for space research - the European Space Agency (ESA) in 1975, and the 1990s is the period during which the union began to work more actively and to invest on a larger scale in the development of various own space initiatives and programmes. Some authors argue that the initial impetus for the emergence of the idea around the deployment of a European space policy was prompted by the EU's recent drive to develop the established international Galileo programme for satellite navigation and positioning, considered the first "real" space programme, which is led by the European Union. This programme is essentially a civil Global Navigation Satellite System (GNSS). It started at the European level in 1999 under the direction of a tripartite body composed of the European Space Agency, the European Union and the air traffic certification organization Eurocontrol. The main result that the EU is aiming for with its implementation is to provide very precise navigation and time signals, independent of other existing technological systems.

In parallel, the EU is investing in the creation of other major space projects - the European Geostationary Navigation Overlay Service (EGNOS) and Copernicus. Established in 2009 the EGNOS space programme provides navigation services to aviation, marine and land users by improving the accuracy of the U.S.

On the other hand, the Copernicus space project is considered the largest programme of its kind in the world and is the EU's contribution to the Global Earth Observation System of Systems (GEOSS). The launch of this space programme took place in 2014 with the launch of its first satellite. The main purpose of the programme is related to the provision of accurate and up-to-date information on Earth orbit observation, and this data should serve in various spheres of, security, defence, and other EU policies.

In the following years, the security and defence aspects of space policy, the security of space infrastructure, the autonomy and access to space and the 'independence' of the European space sector have



expanded in importance. The Commission developed an EU industrial policy for space and created a Space Surveillance and Tracking (SST) and a Government Satellite Communications (Govsatcom) programme.

The influence of space technologies and in particular of the aforementioned satellite systems and their huge revolutionary technological contribution with respect to the security and defence sector of the EU find their legal reflection in a number of legal sources of integration law.

First of all, this is the one created in 2016 **Europe's Space Strategy**[16] If until now the political attitudes of the EU regarding outer space as a separate strategic sector for the Union are textually and regulatorily scattered in various supranational legal documents among other more general policies against the background of the more global political picture, then with the presented on 26.10.2016 space strategy, the first real step has been taken to systematize the Union's political guidelines regarding the space sector. In parallel with this, in relation to it, it is aimed to synchronize the efforts of the member states in this direction. In this sense, this strategy in itself as a legal act represents the first real and tangible attempt to legally frame the European political priorities regarding the space sector. Strengthening the EU's political positions in relation to outer space is of strategic importance, insofar as in this way "its role as a stronger global factor will be strengthened"[16], and on the other hand, the space sector itself is a serious "asset for security and defence of the union." [16] When analyzing the laid down conceptual model of the space policy, it can be established that the same focuses on the realization of the following four main strategic goals: maximizing the benefits of outer space for EU society and economy, fostering a globally competitive and innovative European space sector, strengthening Europe's autonomy in accessing and using outer space in a secure and safe environment and strengthening Europe's role as a global factor and promoting international cooperation. At the same time, with regard to the defence and security of the EU, this space policy pays special attention to the implementation of a series of initiatives and a specific set of regulatory measures oriented in the following directions:

First of all, the space policy prioritizes as a task the preservation of Europe's autonomous access to outer space. Its implementation can be carried out by means of the parallel implementation of the following steps [16]:

1) Deploying modern, efficient and flexible infrastructure facilities by aggregating demand for launch services in order to provide visibility to the industry and reduce implementation costs;

2) Supporting scientific research and innovation efforts, in particular ensuring Europe's ability to respond and accelerate breakthrough changes (reusability, small launch vehicles);

3) Guaranteeing access to radio frequency spectrum;

4) Guaranteeing the protection and sustainability of Europe's critical space infrastructure and ect.

In addition to the above-mentioned space strategy, in 2016 another document important in its legal nature was developed and adopted, namely **A Global Strategy for**

**the European Union's Foreign and Security Policy** [17]. According to some authors such as Chiara Celentino [3] central to this act is the concept of the strategic independence of the EU, which arose in the defence sector and which is perceived as a common driving force of the common foreign and security policy of the union. At the same time, in the substantive dimensions of this concept, the notion that the primary political line that the EU should follow in relation to its defence sector is invariably bound to the fact that the same should have a powerful defence resource is imposed as a conception. The latter, in its turn, implies its constant optimization.

In view of this, in so far as to the achievement of this perspective in the long term are crucial the maintenance of a significant defence capacity and the development of a modernized space equipment, the latter in turn requires the cumulative presence of two prerequisites. The first is related to the process of "synchronization and mutual adaptation of Member States' national defence planning cycles and capability development practices"[3], and the second is aimed at investing in scientific research and technology development in the field of defence. A part from that, a specific prescription for improving European space defence capabilities is introduced in this strategy. It is explicitly stated that the union should emphasize the implementation of the following initiatives: expanding control of flows that have security implications, which requires investment in intelligence data, surveillance and reconnaissance, including remotely piloted aircraft systems, satellite communications, as well as autonomous access to outer space and permanent Earth surveillance.

Currently, these initially formed political guidelines, established by the aforementioned legal acts, have been further developed and upgraded. The evolutionary upsurge of deployment of European legislation in the field of space defence policy is identified with the period of 2019-2024. A series of consistent and significant in their meaning supranational acts have been adopted, which give a clearer and more complete formula for the place occupied by the space defence policy.

**The Regulation (EU) 2021/696 of April 28, 2021 establishing the space programme of the Union and the European Union Agency for the Space Programme**[13], adopted by the European Parliament and the Council, appears to have made a special contribution in the field under consideration. It marks a new stage in the existing up to now European regulatory framework concerning space policy and the space defence industry. Already at the very beginning, stepping on the provision of one of the main founding treaties - Article 189, paragraph 2 of the Treaty on the Functioning of the European Union (TFEU) and after taking into account the increased influence of the space industry and related technological innovations in the fields of digital, information and communication technologies on the EU defence sector, the regulation assigns a special place to the newly created space programme covering the period from 2021-2027 and the main strategic objectives laid down in it in relation to the use and development of the space industrial technological base in relation to the aforementioned sector and which objectives are strongly influenced by the revolutionary decisions of the „Horizon Europe“ programme. On the one hand, the ementioned

space regulation provides a differentiation of the majority of types of activities related to the space industry, subdividing them into "upstream activities" aimed at "creation, development, operation, etc. of an operational space system"[13] and "downstream activities" related to the provision of services and products to outer space" [13].

The developed space technologies in the civil sphere are mainly "dual –use", i.e. they possess the potential of defensive actions and vice versa. In reality, space assets and infrastructure serve both non-governmental and governmental, civil and military purposes, and the proposed programme aims to achieve a systematization of all the regulatory rules that regulate them. On the one hand, the use of this rule-making approach of the European legislator to apply the same rules will help to consolidate the legal framework for all space programmes, and on the other hand, it leads to the facilitation and synchronization of the process of managing European space activities.

In the light of the above, through the above-mentioned supranational act and its direct legal force in relation to the defence sector of the union, the space policy pursues and prioritizes the achievement of more general and additional strategic goals, which in the most synthesized form are the following:

- 1) Enhancing international cooperation, "beneficial interactions" or interpenetration between space activities and activities related to the security and defence of the Union and its Member States;
- 2) Increasing the safety and security of both the union and its member states;
- 3) Ensuring the sustainability of the EU in the conduct of all activities in outer space related to the distribution of space objects and space debris, as well as the space environment;
- 4) Ensuring the security and technological independence of the union, including in the long term for the infrastructure equipment components;
- 5) Taking into account the essential security interests of the Union, an autonomous, secure and cost-effective capability to access outer space is supported;
- 6) Exploiting synergies between civil industry and defence industry, taking into account the security interests of the respective partners and their allies and ect.

For the realization of the same in a long-term plan, the regulation has explicitly provided precisely defined specific priorities and measures. The implementation of the majority of them is closely related to the services available to the navigation satellite systems created so far, such as Galileo, Copernicus, EGNOS, SSA, GOVSATCOM. In relation to the same, the regulation provides, along with the mandatory legal definitions of some key basic concepts in the field under consideration envisaged in the provision of Art. 4 [13] ,explicit definitions of the above-mentioned space programmes with the rule of Art. 3. It has also provided a detailed explanation of their technological nature and functions. Among them, the following stand out with a

priori/emphasized importance in terms of the EU's Security and Defence Policy:

a) for Galileo and EGNOS: to provide long-term, state-of-the-art and secure positioning, navigation and timing services whilst ensuring service continuity and robustness;

b) for "Copernicus": to deliver accurate and reliable Earth observation data, information and services integrating other data sources, supplied on a long-term sustainable basis, to support the formulation, implementation and monitoring of the Union and its Member States' policies and actions based on user requirements;

(c) for SSA: to enhance capabilities to monitor, track and identify space objects and space debris with the aim of further increasing the performance and autonomy of capabilities under the SST sub-component at Union level, to provide SWE services and to map and network Member States' capacities under the NEO sub-component;

d) for GOVSATCOM: to ensure the long-term availability of reliable, secure and cost-effective satellite communications services for GOVSATCOM users.

Last but not least in terms of importance within the framework of the aforementioned regulation is related to the transformation of the European GNSS Agency (GSA) into the European Union Agency for the Space Programme (EUSPA).

In March 2022, the Union's subsequent guidelines regarding space policy were reflected in another supranational act that is significant in its legal nature, namely the so-called **The EU's strategic compass [20]**. Defined by most authors as a "cornerstone" of the European Security and Defence Policy, the Strategic Compass is a comprehensive and up-to-date analysis of the European strategic security environment and the reforms implemented by the Union in this direction. A part from that with the Strategic Compass, in so far as the same is "based on the defence and space packages" [20], the formation of a general strategic vision for an integrated approach in the defence sector, in which clear and precisely defined goals are present, is envisaged as an innovation. In this regard, it should be pointed out that the compass was adopted with the understanding that the effective implementation of the unified defence concept of the union laid down by it is dependent also to a large extent on the global implementation of the same and related recommendations, measures and initiatives. At the same time, against the background of the "shared assessment of the strategic context of the European Union"[20] thus provided with the Strategic Compass and the envisaged "coordinated cooperation in the field of security and defence with the new ways and means to improve European collective defence capabilities set forth in it"[20], the proposals related to the space defence industry stand out. The latter are aimed both at upgrading and supplementing the existing up to now regulatory framework through the creation of a specialized legal act in the field of "EU space policy for security and defence"[20], thus it is revealed that the priority for the union in the long term is the implementation of a strengthened common and consistent approach to

investing in "emerging and disruptive technologies in the field of security and defence."

The Union's main political commitment regarding the defence space technological and industrial base will be tied to increasing its defence capacity and military capabilities by increasing financial means in the direction of developing and improving technologies, ensuring the necessary interaction between civil, military and space industry and exploring opportunities for cooperation with NATO.

Taking into account the fact that "space assets are under civilian control", the EU will put particular emphasis on investing in "dual-use technologies", scientific research and innovation, and in particular one of these future projects will be related to the construction of a "EU space-based global secure communication system in outer space"[19].

The development of "dual-use technologies" was also influenced by the **"Roadmap on critical technologies for security and defence"**[18] adopted during the same period. Taking into account the existence of a legislative gap in integration law regarding the lack of regulatory framework, the European Commission is preparing in 2022 the so-called "Roadmap on critical technologies for security and defence" as the EU's response to curbing strategic dependencies on similar type of technology. At the same time, its main purpose is aimed at forming a unified strategic approach both with regard to the promotion of dual-use Scientific Research, Technological Development and Innovation (SRTDI) at the EU level, and to the identification and acquisition of breakthrough and basic technologies. It also aims to synchronize standards between the civil, defence and space industries through the adoption of some common standards and the creation of a specialized body in the field of critical technologies, namely the Observatory of Critical Technologies.

### III. RESULTS AND DISCUSSION

The adoption of the **European Space Strategy for Security and Defence** [19] is a high point in the evolutionary development of space defence policy. Its creation marks a new turning point in the legislative process of the EU, in so far as it is the first strictly profiled supranational act in the field of the matter under consideration by it, with which, on the one hand, an attempt is made to introduce the most complete systematization for the created until now original set of EU rules and political guidelines laid down in this direction. On the other hand, the aim is to achieve systematization and upgrading of the existing up to now institutionalized form of interaction of space information exchange by means of "expanding the existing mechanism for responding to space threats"[19].

In the light of the foregoing, it can be reported that this space strategy of the EU in the field of defence and security is a significant achievement for European legislation, insofar as through the same is pursued the achievement of the unification of all legal instruments for the protection of the EU's space assets. Because of this, its legal value is huge. This strategy marks a "paradigm shift aimed at strengthening European resilience in and from

space"[11] It helps bridge the existing "gap between space and defence, breaking down silos and strengthening the EU's flagship programs in space for security and defence purposes." [11]

In an interpretive analysis of this document, it can be established that its very title clearly testifies to the specificity of the issues regulated by it. Its main part is an expanded catalog of all a priori political directions in which the union wishes to invest and further develop. In order to improve its space defence capabilities and maintain the permanent "technical sovereignty" of its space industrial base most of the policy guidelines incorporated in it are fully adapted from the Strategic Compass and directly refer to it. On the other hand, it introduces a number of specific authorizations ahead of their time, such as the development of a road map for future innovations in order to reduce strategic dependencies on technologies and increase the competitiveness of the EU's space industry.

In its most synthesized form, the European Space Strategy for Security and Defence focuses on the implementation of the following package of measures and tasks: a set of actions covering the protection of space systems and services, use of space for security and defence; a coordinated response to space threats and seeking to strengthen existing space security cooperation for responsible behavior in space. In this sense, the main concept on which this strategy is built is related to the deployment of these five main pillars of development [9], which in schematic form look like this:



Fig. 1. the five main pillars of development [9]

#### I. Achieving a Shared Understanding of Space Threats.

1) The strategy outlines counterspace capabilities and the main threats in outer space that put space systems and their ground-based infrastructure at risk, relying on a common definition of the space domain. In order to increase the strategic understanding of threats in Member States, the High Representative is tasked with producing a confidential annual analysis of space threats at EU level, using intelligence information provided by Member States.

II. Increasing impact resistance and protection of space systems and services in the EU. In this regard, the space strategy emphasizes the implementation of the following package of measures:

1) A proposal for the development of a European project specialized in the matter under consideration, a legal act - a law on outer space, which should create in global terms a more general legal framework for security, safety and sustainability in space;

2) Formation of a new structure Information Sharing and Analysis Center (ISAC);

3) In the long term, activities are envisaged in connection with the provision of autonomous access of the EU to outer space, emphasizing the needs in the field of security and defence;

4) Strengthening the EU's technological sovereignty by reducing strategic dependencies and ensuring security of supply in the field of space and defence, in close cooperation with the European Defence Agency and the European Space Agency and ect.

III. Strengthening the EU's collective ability to respond to any space attacks and threats that put the EU's security interests at risk

1) Strengthening the "space threat response architecture" and expanding the field of application of the existing up to now response mechanism in view of threats in outer space

2) Better detection and identification of space objects through access to information to create awareness of the space domain through relevant national space commands in order to characterize inappropriate ways of on-orbit behaviors and protect EU assets;

3) Conducting space exercises, including with partners, to test and further develop the EU's response to space threats and explore solidarity mechanisms and ect.

IV. Improving the use of outer space for security and defence purposes

1) Developing concepts for the use of outer space in operational engagements in the line of operations under the Common Security and Defence Policy (CSDP);

2) Development of dual-use space capabilities, including for security and defence purposes;

3) European autonomous capability to provide products and services resulting from exploitation;

4) Space assets and related data to support the autonomous decision-making process of the EU and its Member States and ect.

V. Fostering Global Partnerships in the field of security and defence in outer space.

1) The strategy focuses on building and developing the forms of international cooperation, and in particular, strengthening the partnership with the United Nations and the United States is envisaged and ect.

The European Space Strategy for Security and Defence proposes an ambitious regulatory framework to protect the EU's space assets and protect its interests, deter hostile activities in outer space and strengthen its strategic

position and autonomy. It is characterized by a number of innovations. The first distinguishing mark of the same is related to the fact that there is an acceleration and facilitation of the process of transforming the existing up to now civil space policy and its remodeling to one with certain military applications - clearly taking into account the fact of the "dual nature" of space assets. The second distinguishing mark is aimed at establishing a lasting trend towards the constant and progressive expansion of the circle of exchange of different types of services and data provided by different revolutionary technologies and innovations in relation to the EU defence sector. The third distinctive feature that characterizes this document is related to the envisaged possibility of adopting/laying/affirming a basic line for the cooperation of the EU member states and the protection of its space assets. Parallel to this legislative level, coherence is also envisaged in the implementation of national space defence strategies. In this way, the aim is to strengthen the synchronization and convergence of the European partners in terms of developing a common consistent process of a unified space strategy implemented by them.

#### IV. CONCLUSIONS

After three decades of strong economic interdependence, which was supposed to reduce tensions, the return to power politics and the manifestation of armed aggression is the most significant change in international relations. Maintaining a high-tech defense industrial base is among the a priori goals that European Union sets for itself in its military policy. The space defence policy of the European Union is going through a long and complex evolutionary process of development. The improvement of the legal framework of the space sector by means of the various legal acts/instruments adopted at the supranational level in this direction is an important step for the creation of a common vision for space collective defence and the application of uniform standards regarding related space technology, data and services in the defence sector. This, in turn, will lead to an increase in the defence capacity of the Union and to the confirmation of its leadership role in the defence sector among other global actors against the background of the international political scene. Investing in Europe's sovereign space infrastructure, maintaining European leadership and leveraging industrial and scientific expertise in space in the long term is of utmost importance for the European Union, as it will enable a collective defence capability of the Union to be able to respond the challenges today and anticipate the needs of tomorrow.

#### REFERENCES

- [1] T. Dimitrov, "Legal and ethical principles as a regulatory basis of the effect of artificial intelligence in the field of security and defence", Report at a scientific conference with participation "Shared sustainability of international South-Eastern Europe", BA "G. S. Rakovski", 2023, Military Journal 2023, 2023, no. 3, pp. 239 – 249, ISSN: 0861-7392R.
- [2] Muñoz and C. Portela, "The EU Space strategy for security and defence: towards strategic autonomy?", № 83, June 2023, EU Non-Proliferation and Disarmament Consortium, non-proliferation and disarmament papers, [Online], Available: [https://www.sipri.org/sites/default/files/2023-06/eunpdc\\_space\\_paper\\_no\\_83\\_0.pdf](https://www.sipri.org/sites/default/files/2023-06/eunpdc_space_paper_no_83_0.pdf), [Accessed: Jan. 21, 2024].
- [3] C. Cellerino, "EU Space Policy and Strategic Autonomy: Tackling Legal Complexities in the Enhancement of the 'Security and Defence Dimension of the Union in Space'", European Papers, Journal, Jul 27, .2023, [Online], Available:

- <https://www.europeanpapers.eu/en/authors/chiara-cellerino>, [Accessed: Jan. 21, 2024]
- [4] European Court of Auditors, EU space programmes Galileo and Copernicus: services launched, but the uptake needs a further boost, Special report Europe's space assets, Jul, 2021, [Online], Available: <https://op.europa.eu/webpub/eca/special-reports/space-programmes-7-2021/en/>, [Accessed: Dec 16, 2023].
- [5] G. Perotto, "The Legal Framework of the EU Defence Industry and the Pursuit of Strategic Autonomy", European Papers, Journal, Jul 27, 2023, [Online], Available: <https://www.europeanpapers.eu/en/authors/gabriella-perotto>, [Accessed: Jan. 7, 2024].
- [6] G. Penchev, "Legal regime of the access to information under secondary law of the European Union: general problems with indirect meaning for the protection of the environment", Nov 28, 2021, [Online], Available: <https://www.challengingthelaw.com/ekologia/praven-rejim-dostap-informaciya-pes/>, [Accessed Dec 20, 2023]
- [7] Think Tank European Parliament, "European space policy: Historical perspective, specific aspects and key challenges", In-Depth Analyzis, Jan 30, 2017, [Online], Available: [https://www.europarl.europa.eu/thinktank/en/document/EPRS\\_ID\\_A\(2017\)595917](https://www.europarl.europa.eu/thinktank/en/document/EPRS_ID_A(2017)595917), [Accessed: Dec 20, 2024].
- [8] V. Reillon, "European space policy; Historical perspective, specific aspects and key challenges", Jan 31, 2017, [Online], Available: <https://epthinktank.eu/2017/01/31/european-space-policy-historical-perspective-specific-aspects-and-key-challenges/>, [Accessed Sept 23, 2023]
- [9] European Space Policy Institute ESPI, "High time for an EU Space Strategy for Security and Defence", Brief № 63, Mar 10, 2023, [Online], Available: <https://www.espi.or.at/wp-content/uploads/2023/03/ESPI-Executive-Brief-n%C2%B063-March-2023-final.pdf>, [Accessed: Jan 25, 2024].
- [10] European commission, "An EU Space Strategy for Security and Defence to ensure a stronger and more resilient EU", Mar 10, 2023, [Online], Available: [https://ec.europa.eu/commission/presscorner/detail/bg/ip\\_23\\_1601](https://ec.europa.eu/commission/presscorner/detail/bg/ip_23_1601), [Accessed: Dec 10, 2023]
- [11] European union, European union Space Strategy for Security and Defence for a stronger and more resilient European Union, [Online], Available: [https://defence-industry-space.ec.europa.eu/eu-space-policy/eu-space-strategy-security-and-defence\\_en](https://defence-industry-space.ec.europa.eu/eu-space-policy/eu-space-strategy-security-and-defence_en), [Accessed: Dec 10, 2023]
- [12] European Parliament, Resolution on the European space policy: how to bring space down to earth, [Online], Nov 20, 2008, Available: [https://www.europarl.europa.eu/doceo/document/TA-6-2008-0564\\_BG.html](https://www.europarl.europa.eu/doceo/document/TA-6-2008-0564_BG.html), [Accessed: Dec. 19, 2023].
- [13] Regulation (eu) 2021/696 of the European parliament and of the Council of establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU, April 28, 2021, Available: <https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32021R0696>, [Accessed: Dec. 16, 2023].
- [14] The Treaty on the Functioning of the European Union (TFEU), Article 2, Official Journal of the European Union, C 202/1, Jun 7, 2016, [Online], <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12016ME%2FTXT>, [Accessed: Dec 4, 2023]
- [15] United Nations, Charter of the United Nations and statute of the International court of justice, 1945, [Online], Available: <https://treaties.un.org/doc/publication/ctc/uncharter.pdf>, [Accessed: Dec 11, 2023].
- [16] European commission, Communication from the commission to the European parliament, the Council, the European economic and Social committee and the Committee of the regions Space strategy for Europe, COM/2016/0705 final, Oct 10, 2016, [Online], Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2016%3A705%3AFIN>, [Accessed: May 15, 2023].
- [17] European Union, A Common foreign and security policy — Global strategy, Global Strategy for the European Union's Foreign And Security Policy, 2016, Sept 08, 2020, [Online], <https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=LEGISSUM:4413648>, [Accessed: Oct 15, 2023]
- [18] European commission, Communication from the commission to the European parliament, the Council, the European economic and social committee and the Committee of the regions Roadmap on critical technologies for security and defence, Com/2022/61 final, Mar 15, 2022, [Online], Available: <https://eur-lex.europa.eu/legal-content/en/txt/?uri=celex%3a52022dc0061>, [Accessed: Dec 18, 2023].
- [19] European commission, Joint communication to the european parliament and the Council European Union Space strategy for security and defence, join/2023/9 final, Mar 10, 2023, [Online], Available: <https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A52023JC0009&qid=1708802913760>, [Accessed: Dec 17, 2023].
- [20] Council of the European Union, A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security, Mar 21 2022, [Online], Available: <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf>, [Accessed: Jan 25, 2024].

# *Legal Approach To Implementing Security Measures For Combatting Threats To National Critical Infrastructures*

**Maria Neikova**

*Department of National Security  
University of Library Studies and  
Information Technologies  
Sofia, Bulgaria  
m.neykova@unibit.bg*

**Abstract.** The quality of life and security of all citizens, including all EU citizens, is closely related to the provision of essential services through interaction of different critical infrastructures. Cross sectoral measures are required to be implemented in order to obtain high level of protection and optimal minimisation of potential risks for critical infrastructures, as various potential risks could also affect national security.

Taking into account the fact that the general framework on critical infrastructure sometimes could not sufficiently address all various challenges to critical infrastructures in each and every country, it is possible to consider complex legislative approach for implementation of security measures for combatting threats to national critical infrastructures.

The current articles outlines the specifics of implementing legal approach in reference to combatting threats to national critical infrastructures in line with the EU regulatory framework and focusing also to Bulgarian national legal sources and practical challenges.

**Keywords:** *complex measures, critical infrastructure, national security, legal framework.*

## I. INTRODUCTION

Examining the current developments and future challenges facing international, European and Bulgarian essential national infrastructures entails a comprehensive understanding of diverse issues, including cyber security risks, the impact of geopolitical dynamics, the effects of climate change, and financial stability, among other factors. Bulgaria, as a country situated at the crossroads of Europe and Asia, faces several unique challenges in protecting its critical infrastructure. Some of the primary elements forming key factors having the potential to affect critical infrastructures' stability include: cyber threats,

geopolitical factors, environmental factors and climate change, environmental degradation, factors causing economic instability, migration and corruption practices. [1, 2]

The theoretical basis for securing critical infrastructures against diverse threats starts with a deep understanding of the inherent vulnerabilities and risks these essential assets face. These infrastructures, which include utilities like electricity and water, as well as telecommunications systems, are crucial for national security and public welfare, necessitating their protection.

The core theoretical model integrates principles from risk management, which advocates for a methodical approach to identifying, evaluating, and mitigating risks. It also incorporates resilience theory, emphasizing the strengthening of these systems' capacity to endure and bounce back from disruptions. This comprehensive perspective ensures that strategies not only focus on preventing threats through stringent security measures but also on recovering swiftly from incidents.

The legal framework component relates to the application and effectiveness of laws and regulations that are designed to protect infrastructure. This involves a detailed approach to both national and international legal provisions facilitating understand enforcement mechanisms and ensure compliance across all parties involved.

Conducting a thorough examination to understand the specific aspects of safeguarding national critical infrastructure involves exploring the core principles behind its protection. This includes looking into the identification of security practices against potential threats, understanding the system's susceptibilities, evaluating risks, devising defence strategies, and recognizing the

*Print ISSN 1691-5402*

*Online ISSN 2256-070X*

<https://doi.org/10.17770/etr2024vol4.8240>

© 2024 Maria Neikova. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

mutual dependencies within the infrastructure system, in addition to outlining the relevant policy frameworks and governance structures. Ensuring the safety of vital infrastructure and the strength of the entities that manage these systems is crucial for the functioning of society. Our daily lives depend heavily on uninterrupted access to essential services such as energy, clean water, healthcare, financial services, and reliable transportation systems.[3]

Consequently, the European Commission has been proactive in promoting the safeguarding of critical infrastructure and enhancing the durability of essential services against both natural disasters and human-induced threats.

## II. MATERIALS AND METHODS

The European Union has developed a comprehensive strategy for enhancing the security and resilience of vital infrastructures through the European Programme for Critical Infrastructure Protection (EPCIP), initiated in 2006 following the Commission's Communication on Critical Infrastructure Protection in the context of counter-terrorism efforts. This programme enables the Commission to:

- Encourage collaboration among European Union (EU) Member States and with international counterparts, including the United States, Canada, countries in the Western Balkans, and Eastern Europe.
- Assist Member States in strengthening the resilience of essential services and infrastructure.
- Allocate funding for research, studies, and projects related to critical infrastructure protection. Significant funding avenues include contributions to the security research programme under Horizon Europe and support for the European Reference Network for Critical Infrastructure Protection (ERNICIP).

In response to the necessity for enhanced measures for supporting and protect EU's vital infrastructure, in 2022 a Council Recommendation has been adopted, which sets forth a Union-wide collaborative effort to boost critical infrastructure resilience.[4] This recommendation delineates three core focus areas: enhancing preparedness, improving response mechanisms, and fortifying international collaboration. To improve preparedness, it suggests Member States refresh their risk evaluations to mirror current threats and undertake stress tests grounded on shared principles and collective scenarios at the EU level, initially focusing on the energy domain. Regarding response capabilities, it advocates for the creation of a Blueprint for a unified reaction to disruptions affecting critical infrastructures with notable cross-border impacts. The initiative follows the resilient infrastructure five-point strategy introduced, as it encourages EU Member States to increase their readiness and countermeasures against prevailing threats. This involves both preliminary actions aligned with the forthcoming Critical Entities Resilience Directive and the employment of supplementary tools in a synergized fashion.[5]

The practical implementation of security measures for critical infrastructure follows a systematic process, beginning with an in-depth risk assessment to pinpoint potential threats and their impacts. This assessment informs the development of customized security strategies that include physical and cyber defences tailored to the identified risks.[6]

The Commission has also put forward a proposal for a Council Recommendation on this Blueprint, which is currently under deliberation with Member States. Moreover, amplifying international cooperation, notably with NATO and principal ally nations, is envisaged to effectively tackle risks and incidents of significant cross-border concern. An EU-NATO Task Force dedicated to the resilience of critical infrastructure has been initiated, producing an evaluative report with pertinent recommendations in this domain. [7]

## III. RESULTS AND DISCUSSION

The entities involved in the provision of essential services are increasingly subject to diverging requirements imposed under national law. The fact that some Member States have less stringent security requirements on those entities not only leads to various levels of resilience, but also risks negatively impacting the maintenance of vital societal functions or economic activities across the Union and leads to obstacles to the proper functioning of the internal market.[8]

In that regard, from Legal and Regulatory Perspective, the European Commission introduced in 2020 a proposal for Directive on the resilience of critical entities. The Directive has been adopted since the end of 2022.

The Directive does not affect the competence of Member States and their authorities in terms of administrative autonomy or their responsibility for safeguarding national security and defence or their power to safeguard other essential State functions, in particular concerning public security, territorial integrity and the maintenance of law and order. [9]

The exclusion of public administration entities from the scope of this Directive should be applied to entities whose activities are predominantly carried out in the areas of national security, public security, defence or law enforcement, including the investigation, detection and prosecution of criminal offences. However, public administration entities whose activities are only marginally related to those areas should fall within the scope of this Directive.

With a view to ensuring a comprehensive approach to the resilience of critical entities, each Member State should have in place a strategy for enhancing the resilience of critical entities.

At an European Union level, there have been established process mechanisms for identifying and designation of European Critical Infrastructures. The legal framework also sets out an approach for improving the protection of critical infrastructures. To address these concerns, the European Commission put forward a Directive proposal in 2020 aimed at enhancing the resilience of critical entities, which has been in effect since late 2022. This Directive respects the sovereignty of

Member States regarding their administrative autonomy and their duties to protect national security, defence, and other critical state functions, particularly in areas related to public security, territorial integrity, and maintaining public order. It specifies that entities primarily engaged in national security, public security, defence, or law enforcement activities, including criminal investigations and proceedings, are exempt from its provisions. Nonetheless, entities with only minor connections to these sectors are included within its scope. [10]

To foster a holistic approach to bolstering the resilience of critical infrastructures, the Directive mandates that each Member State develops a strategic plan to strengthen such entities. Furthermore, at the EU level, processes and mechanisms have been put in place for identifying and designating European Critical Infrastructures, alongside establishing methodologies to improve the protection of these infrastructures.

#### IV. CONCLUSION

Identification and designation of European critical infrastructures required the EU countries Member States to go through a process of identifying potential critical infrastructures along with guidance and support provided by the European Commission. It is specifically important that identifying potential critical infrastructures, Member States should use cross-cutting criteria (such as possible casualties, economic effects and effect on the public), as well as sectoral criteria for identification, which criteria are specific according to the type of critical infrastructure being identified. In that regard, each and every European Union Member State has to go through a cooperative designation process for potential European Critical Infrastructure detection located on its territory.

In Europe, including Bulgaria, the safeguarding of national critical infrastructures is guided by a mix of overarching EU directives and specific national legislations that adhere to these European norms. The European Union has laid down a detailed legal structure to boost the resilience and safeguarding of crucial infrastructures throughout its member states. The concept of National critical infrastructure, encompasses the essential physical and cyber-based systems and assets whose failure or incapacitation could severely affect national security, economic well-being, public health, or safety. This broad category covers various sectors and components crucial for a nation's functioning and security.

Bulgaria, as a member of the EU, complies with these regulations, embedding them within its national framework for critical infrastructure protection. This involves transposing EU directives into national law and enacting specific protective measures to address the country's unique challenges and vulnerabilities within its critical infrastructure sectors. This cohesive approach between EU-wide directives and national legislation strives to establish a comprehensive and resilient framework for the protection of critical infrastructure across Europe, enabling coordinated responses to a wide range of threats.

Bulgaria's strategic emphasis on enhancing the resilience and security of its essential services and infrastructures is critical given its geographic significance and aspirations to integrate further into the European

Union's Schengen zone. This focus is particularly vital against the backdrop of global challenges and regional instabilities.

According to national regulations in Bulgaria the process of establishment of a potential European critical infrastructure at the territory of the Republic of Bulgaria, at an organizational level has to be carried out by a certain minister – member of the Council of Ministers. The exact procedures for the establishment and designation of European Critical Infrastructure on the territory of the Republic of Bulgaria, as well and the measures for their protection shall be determined by an ordinance of the Council of Ministers. [11]

As of 2013, Bulgaria has adopted an Ordinance on the procedure for the establishment and designation of European critical infrastructures in the Republic of Bulgaria and the measures of their protection. According to the legislative provisions and definitions set from regulatory aspect, the term Critical Infrastructure, according to the Ordinance includes an entire system or parts of it that are essential for maintaining vital social functions, health, safety, security, economic or social well-being of the population and whose violation or destruction would have significant negative consequences for the Republic of Bulgaria as a result of the inability to be retain these features.

#### V. FUTURE PERSPECTIVES

Addressing future challenges to national critical infrastructures requires a legal strategy that encompasses strong regulatory frameworks and comprehensive policy initiatives. Organizations responsible for delivering essential services across the EU are facing a patchwork of national regulations that often differ in stringency. This disparity in security standards among Member States not only creates levels of resilience but can also affect the continuous operation of crucial societal functions or economic activities throughout the Union.

Strategic guidelines and activities should support the development and implementation of laws and policies aimed at safeguarding the interconnected systems of security mechanisms, operational technologies and information technologies, recognizing the potential risks which could occur related to integration processes conduction. [12]

The legal framework needs to adapt to the changing landscape. Furthermore, enhancing the security and resilience of critical infrastructure requires legal support for efforts to collaborate with both public and private sectors. This includes intelligence sharing, vulnerability assessments, technological investments for protection, and other services aimed at strengthening the resilience of the nation's critical infrastructure against a spectrum of threats.

Tackling future threats to national critical infrastructures from a legal viewpoint involves reinforcing legal structures, enhancing international partnerships, and employing proactive security and policy measures.

#### REFERENCES

- [1] Deliversky, J., *Illegal Migration and Refugee Crisis as a Threat to National Security, Economic and Social System - The Bulgarian*



- Case, Journal of educational and instructional studies in the world, May 2018, vol. 8, issue 2, 47-50
- [2] Zahariev, M. Legal guarantees for the security of personal data processed by the competent authorities for law enforcement activities, [in Bulgarian], Collection of Reports, National Scientific Conference with International Participation "Security and Defense", Academic Publishing House "Za Bukvite – O Pismeneh", Sofia, 2023, c. 492-506, ISBN 978-619-185-593-3.
- [3] 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, OJ L 333, 27.12.2022, p. 164–198
- [4] European Commission, Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM(2006) 786 final [accessed March 15, 2024]
- [5] Angelov, G., Model for developing a strategy for protecting national security [in Bulgarian], Legal Collection, Burgas Free University, Center for Legal Studies, Volume XXIX, pp. 46-53, ISSN 1311 – 3771
- [6] European Commission, EU-NATO Task Force on the resilience of critical infrastructure, Final Assessment Report, June 2023
- [7] European Commission, Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities. Explanatory memorandum, COM (2020) 829 final [accessed March 15, 2024]
- [8] Council 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 (OJ L 345, 23.12.2008, pp. 75–82)
- [9] Ordinance on the procedure for the establishment and designation of European critical infrastructures in the Republic of Bulgaria, adopted by Decree No. 38 of 18.02.2013, promulgated in State Gazette issue 19 of 26.02.2013
- [10] Ordinance on the procedure for the establishment and designation of European critical infrastructures in the Republic of Bulgaria, adopted by Decree No. 38 of 18.02.2013, promulgated in State Gazette issue 19 of 26.02.2013
- [11] Deliversky, J., Open access and human rights of refugees in the context of world migration processes [in Bulgarian], Proceedings book - 5th National seminar with international participation, UNIBIT, 2017, pp. 221–230., ISBN 978-619-185-272-7
- [12] Council 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 (OJ L 345, 23.12.2008, pp. 75–82)

# *Application of Software Platforms to Enhance Early Warning and Detection System Capabilities for Nuclear Weapons Threat*

**Nikolay Iliyanov Padarev**

„V. Levski” National Military University  
Faculty of Security and Defence  
Veliko Tarnovo, Bulgaria  
[nipadarev@gmail.com](mailto:nipadarev@gmail.com)

**Abstract.** The report describes the potential damage from the striking factors of low- and medium-yield nuclear munitions. A scenario of a terrestrial nuclear explosion in a city is modelled. Analytical calculations are proposed for nuclear blast damage for which no simulation platform is implemented. An analysis was made of the damage to residential buildings and the population from the light pulse, radiation pollution through a software platform. Data for the electromagnetic pulse area are extracted. A comparison was made of the sizes of the damage zones for the striking factors of the nuclear weapon in the respective powers of the nuclear explosion.

**Keywords:** weapons of mass destruction, nuclear event warning, simulation platforms, early warning.

## I. INTRODUCTION

Military science has always been very concerned that effects and protection of radioactive substances. Nuclear events are among the most dangerous events possible. They result in injury and death to exposed persons, destruction of property and long-term risks to both populations exposed to event and those exposed to its consequences, e.g. radioactive waste. Nuclear events cause a combination of damage due to the rapid nuclear effects—radiation, pressure, and heat energy that result from the detonation. [1], [2] According to the environment in which nuclear events occur, we can classify them as radiological events in facilities (from the Interpretive Dictionary of the Bulgarian language - "a building with a specific purpose") and outdoors. The aim of this development is to propose a tool for the rapid evaluation of radiological events in facilities. [3], [4]

Artificial intelligence applications have been implemented more frequently in recent years due to their potential to reduce costs and reliability. Software platforms have a lot of advantage in security and defence

training. Nowadays, there is an increasing interest in protection against nuclear, radiological, chemical, and biological events. [3], [4], [5]

Military software applications have the advantage of creating a dangerous virtual environment and verifying training and knowledge before participating in field exercises and actual combat operations. [2], [6].

Predicting the overwhelming effect of a nuclear weapon is a fragment of the warning to military troops and population in nuclear incidents. [7], [8] Nuclear events are among the most dangerous events possible. They result in injuries and deaths to exposed persons, destruction of property and long-term risks to both populations exposed to the event and those exposed to its consequences, e.g. radioactive waste. Nuclear events cause a combination of injuries due to the rapid nuclear effects—radiation, blast overpressure, and thermal energy—as a result of detonation. In addition, there are secondary effects (collapse and collapse of buildings due to secondary, tertiary, and quaternary dynamic pressure) and indirect effects (lightning blindness and burns due to secondary fires) that result from the detonation. The purpose of this development is to provide an answer for the damage zones resulting from detonation of a nuclear weapon through geospatial analysis, to protect the population and infrastructure and planning their evacuation. Nuclear explosions of 20 kt TNT and 50 kt TNT are taken as a limit for the study.

## II. MATERIALS AND METHODS

The study is a simplified concept of risk definition and analysis that assesses not probability, but rather spatial exposure and known degrees of hazard magnitude from existing tactical nuclear warheads.

Print ISSN 1691-5402  
Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8202>

© 2024 Nikolay Iliyanov Padarev. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

The software platform "Nukemap" used for calculation of damage from nuclear weapons allows users to carry out in spatial planning or protection of the population with a simplified model for making assessments in areas of responsibility. In the present study, we also use the software product HotSpot Version 3.1.2. Terrestrial nuclear explosions of 20 kT and 50 kT TNT are taken as constraints for the study.

To achieve the stunning effect of a nuclear explosion, the detonation can be air or ground. Terrestrial nuclear explosions (NWs) [9], [10] are primarily chosen to exploit heat shock and maximum radiation contamination. Exposure ranges for typical nuclear weapons are chosen continuously with a 50% fission rate estimate and a 30 km/h wind speed [11]. For the effects of radioactive substances, weight ranges of 0,1 Gy and above have been chosen, which lead to severe damage to health.

### III. RESULT AND DISCUSSION

Visually, the results are displayed on map bases that depict the strike zones of hypothetical nuclear attacks. The main goal of the research is to predict the dangerous factors of a nuclear attack with software platforms to be used in the early warning system in the Republic of Bulgaria. The choice of nuclear blast power is also arbitrary but is tailored to what nuclear material can be loaded on a tactical munition/missile.

When assessing the nuclear consequences of small and medium-power nuclear weapons (NW), it is of great importance to assess the damage caused by the shock wave. The distribution and severity of these damages depends on durability of device, height of the blast, meteorological factors, protection parameters by shelter, and specifics of the terrain.

To model the evaluation of blast effects and damage assessment, pressure zones should be analyzed according to the pressure peak, and in this study, a maximum of 50 psi and a minimum of 1 psi were considered [12]. The overpressure of the blast that will cause damage to buildings and the population can vary from 0,5 psi to 50 psi. A burst overpressure of 0,5 psi can shatter window glass and some facades. Pressure of 2 to 3 psi can cause damage to some wood and masonry structures. A blast pressure of 3 psi to 8 psi can cause damage to brick and concrete buildings. Based on the calculated distance from the center/epicenter from NW, the buffer zones can be calculated, and the damage can be estimated according to the pressure created in them. [12]

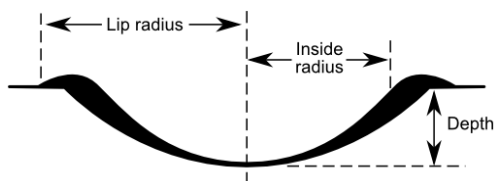


Fig. 1. Crater diagram

TABLE 1 DAMAGE TO PEOPLE FROM THE NW 20 kT SHOCK WAVE

Parameters	20 kT	50 kT
Crater inside radius	52,4 m (0,01 km <sup>2</sup> )	71,1 m (0,02 km <sup>2</sup> )
Crater depth:	25,1 m	34 m

Crater lip radius	105 m (0,03 km <sup>2</sup> )	142 m (0,06 km <sup>2</sup> )
● Heavy blast damage (20 psi)	0,59 km (1.1 km <sup>2</sup> )	0,8 km (2,02 km <sup>2</sup> )
○ Light blast damage (1 psi)	3,19 km (32 km <sup>2</sup> )	4,33 km (59 km <sup>2</sup> )

The extent and severity of the damage and destruction in a NW cannot be predicted with great accuracy, as it largely depends on the environment in which the epicentre/centre of the NW is located - an airport, an administrative centre, an industrial area, etc.

If the barrier is not large, the air shock wave begins to flow around it. The air stream then flows around the baffle as in a strong wind. The transient lasts as long as it takes for the discharge wave and vortex motion to completely cover the barrier. This time  $t_\alpha$  can be approximately calculated as:

$$t_\alpha = \frac{B}{340}, \text{sek} \quad (1)$$

where: B is the width of the partition.

If  $t_\alpha$  is small compared to the time of action of the overpressure, it can be considered that the action of the air shock wave in this case is like a hurricane gust.

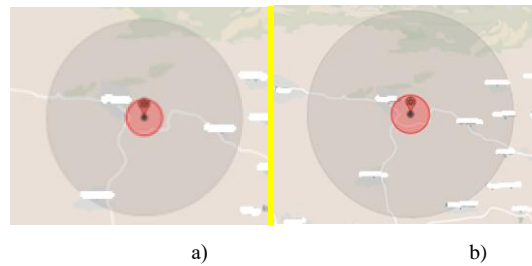


Fig. 2. Zones of impact by the shock wave at the power of the nuclear explosion a) 20 kT and b) 50 kT

In fig. 2 shows the destructive action of the shock wave in two zones, which are concentric circles centred on the site of the nuclear explosion. In real conditions in a populated place or terrain with relief other than flat, perfect concentric circles will not be obtained. Any obstacle in the front of the shock wave will affect their shape. When making predictions for striking action, areas of larger area are always given, i.e. this variant of describing the zones can be accepted as applicable. At 20 psi overpressure, heavily built concrete buildings are severely damaged or demolished: fatalities approach 100 %. Often used as a benchmark for heavy damage in cities. At a around 1 psi overpressure, glass windows can be expected to break. This can cause many injuries in a surrounding population who comes to a window after seeing the flash of a nuclear explosion (which travels faster than the pressure wave). Often used as a benchmark for light damage in cities.

Formula (2) can be used to calculate the overpressure in front of the shock wave in water:

$$\Delta P_{so} = 23000 \frac{\sqrt{W}}{\sqrt{R^3}}, \frac{kg \text{ TNT}}{cm^2} \quad (2)$$

The time of action of overpressure in water is about 130 times less than in air.

$$L = 0.015\sqrt{R}\sqrt[6]{W}, \quad (3)$$

where L, m is water layer thickness for water shock wave front.

For example, at a NW with 20 kt TNT at 1000 m, L=10 m is obtained. [12]. Table 1 shows the impact of peak overpressure on humans (data from HOTSpot software).

TABLE 2. DAMAGE TO PEOPLE FROM THE NW 20 KT AND 50 KT SHOCK WAVE

Lesions / pressure	Distance from the epicenter of the explosion, km at 20 kt TNT	Distance from the epicenter of the explosion, km at 50 kt TNT
<i>Deadly</i>		
more than 30 psi (30–50)	0,50	0,66
50 % 50 psi (50–75)	0,40	0,53
100 % 75 psi (75–115)	0,33	0,45
<i>Lung Damage</i>		
to 8 psi (8–15)	0,94	1,27
pressure 20 psi (20–30)	0,59	0,80
<i>Eardrum rupture</i>		
to 5 psi	1,21	1,64
50 % 15 psi (15–20)	0,68	0,92
<i>Shattered window glass injury</i>		
Threshold 0.5 psi	5,15	6,99

The thermal effects are an important aspect when considering light emission and play a role in different scenarios where heat can cause different effects. In the context of combat equipment and firearms, thermal action can be of particular importance, causing severe damage and destruction. The thermal radiation can also be dangerous in industrial environments where high temperatures or flames can start fires or cause damage to materials. Understanding the thermal characteristics of different materials is important for the safe operation and design of buildings and sites. Also, the distribution of heat in materials depends on their thermal conductivity. The materials such as wood and concrete have lower thermal conductivity, meaning they can retain heat longer than materials such as armor and aluminum with higher thermal conductivity. This factor can be essential in risk analysis and taking measures to prevent or manage heat damage.

In daytime conditions, a 20 kT explosion can cause temporary flash blindness from scattered light at 23 km. Individuals directly looking at the fireball could experience retinal burns at 25 km. Unprotected individuals could receive more than the dose of thermal radiation required for third-degree burns at a distance of up to 1,9 km.

The thermal energy and the corresponding deposition range (radial distances) can be calculated by formula (4):

$$Q \left( \frac{\text{cal}}{\text{cm}^2} \right) = \frac{7.9fwr}{D^2}, [12] \quad (4)$$

where:

- W is power of nuclear weapon, kg TNT;
- D is the distance from the epicentre/centre, km.

- f is the thermal distribution coefficient.
- $\tau$ – permeability of the medium.

The degree to which a person is struck in the zone of heat radiation at NW can be determined by the HotSpot model. (Table 3)

TABLE 3. DEGREE OF SKIN BURN AND EYE INJURY FROM THERMAL RADIATION (SOURCE – HOTSPT)

Hazard	Distance from the epicenter of the explosion, km at 20 kt TNT	Distance from the epicenter of the explosion, km at 50 kt TNT
Eye damage		
Day		
- blindness	23	25
- retinal burns	25	28
Night		
- blindness	75	77
- retinal burns	44	48

With the Nukemap software platform, a simulation of an aerial nuclear explosion with a power of 20 kt TNT was made (Fig. 3). The influence of thermal radiation was investigated.

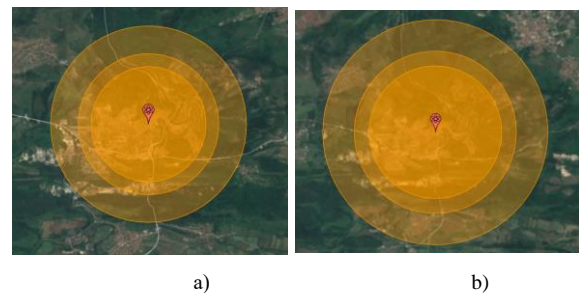


Fig. 3. Zones of impact by the thermal radiation at the power of the nuclear explosion a) 20 kt and b) 50 kt

Third degree burns extend throughout the layers of skin and are often painless because they destroy the pain nerves. They can cause severe scarring or disablement and can require amputation. 50% probability for 3rd degree burns at this yield is 7,57 cal/cm<sup>2</sup>. Second degree burns are deeper burns to several layers of the skin. They are very painful and require several weeks to heal. Extreme second-degree burns can produce scarring or require grafting. 50 % probability for 2nd degree burns at this yield is 4,97 cal/cm<sup>2</sup>. First degree burns are superficial burns to the outer layers of the skin. They are painful but heal in 5-10 days. They are the same thing as a sunburn. 50 % probability for 1st degree burns at this yield is 2,47 cal/cm<sup>2</sup>.

The most significant is gamma–radiation, the presence of which is a danger to humans due to its range and penetrating ability. Residual radiation weakens and scatters in the same way as primary gamma–radiation. The biological effects on humans from residual radiation are the same as for primary radiation. Delayed ionizing radiation is produced by fission products and induced by environmental radionuclides (soil, air, structures, remnants of nuclear devices). These radioactive products will be dispersed to the leeward side. As the cloud moves along the trail, radioactive material that has fallen and settled on the ground creates trails of fallout. Fallout radioactive materials are the dominant source of radiation emission for locations outside the immediate effects of a

nuclear detonation. The dose received depends on the length of time a person remains in the contaminated area.

The study used a Gaussian model of air pollution with radioactive substances through the HotSpot software. In Gaussian models, it is assumed that the spread of the radioactive cloud in vertical and horizontal directions takes place by diffusion along the direction of the mean wind. The reports [13], [14] discusses the health effects and consequences of nuclear weapons, considering the physical, environmental, and medical impacts of nuclear explosions. It may also address the humanitarian aspects of nuclear weapons, advocating for disarmament and emphasizing the need to prevent the use of such destructive weaponry. The maximum concentration at the ground surface is calculated using the following equation:

$$C_x = \frac{Q}{\pi\sigma_y\sigma_z u} e^{-\frac{1}{2}\left[\frac{y}{\sigma_y}\right]^2}, [13] \quad (5)$$

where:

Q – average emission rate, g/s,

U – average wind speed, m/s;

H – effective cloud height, m;

$\sigma_y$  – standard deviation of the wind direction in the horizontal, m;

$\sigma_z$  – standard deviation of the wind direction in the vertical, m;

y – off center distance, m;

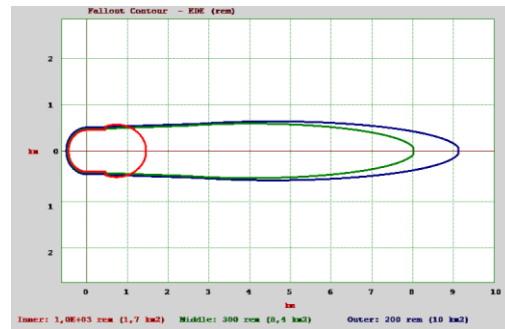
e – natural logarithm = 2,71828.

A hypothetical terrestrial nuclear explosion with a yield of 20 kt and 50 kt TNT was simulated using the HotSpot 3.1.2 software product. Fig. 3 shows a model of the trail of radioactive cloud for a nuclear explosion. A wind speed of 8 m/s has been entered for the purpose of analysis. In the model, a dose of 3,000 rem was fixed for the inner plume, and 300 rem for the outer plume. The intermediate loop was set at 1,000 rem. The software has the ability to assess the defeat of people behind a barrier that will reduce the impact of ionizing radiation. The options available in the software are: unshielded, 1 m underground, house, basement, high-rise building - upper floor, high-rise building - lower floor, location behind concrete wall 22.86 cm, behind concrete wall 30.48 cm and in vehicles (car, bus).

When designing the simulation model, the bottom floor of a multi-storey building is set, the time after the explosion is fixed to one hour. In fig. 3 contours of radioactive contamination are shown. The contours are of three plume layers, coloured in red, green and blue with the correspondingly set doses of radiation.



a)



b)

Fig. 4. Areas of radioactive contamination a) 20 kt and b) 50 kt

Radiation casualties may be caused by prompt nuclear radiation or by radioactive fallout. Unprotected individuals could receive more than the prompt ionizing radiation dose required for 50 % lethality (within weeks), out to 1,5 km for 20 kt nuclear explosion and 1,7 km for 50 kt.

The radioactive products will be dispersed downwind with the fireball/debris cloud. As cloud travels downwind, the radioactive material that has fallen and settled on the ground creates a footprint of deposited material (fallout).

The exposure to fallout is dominant source of radiation exposure for locations beyond prompt effects of nuclear detonation. The dose received depends upon the time an individual remains in the contaminated area. Unprotected individuals remaining in the contamination zone for the first hour following the nuclear explosion could receive more than the fallout dose required for 50 % lethality (within weeks), out to about 12 km for 20 kt NW and 14 km. The idealized maximum width of the fallout footprint (actual width could be larger or smaller) is about 0,56 km for 20 kt yield and 1,64 times more for the 50 kt TNT nuclear explosion. For individuals remaining in the contamination for the first 24 hours, the downwind extent of the 50 % lethality contour increases to approximately 1,37 times at 20 kt TNT vs. 50 kt nuclear blast power. The 50 % lethality contour width increases to about at 20 kt TNT is 1.3 km and at 50 kt nuclear blast power is 2,2 km.

The electromagnetic power (EMP) range for the 20 kt detonation is approximately 5 km, for the 50 kt detonation is approximately too. Indeed, not all equipment in the EMP-effect range will fail. The extent of damage depends on several factors, including proximity to the

source, the size of the equipment's receiving antenna, and its susceptibility to EMP effects. In general, semiconductor devices are more vulnerable to EMP than vacuum tube devices, and smaller antennas are less likely to be affected. Indeed, not all equipment in the EMP-effect range will fail. The extent of damage depends on several factors, including proximity to the source, the size of the equipment's receiving antenna, and its susceptibility to EMP effects. In general, semiconductor devices are more vulnerable to EMP than vacuum tube devices, and smaller antennas are less likely to be affected. Electromechanical devices such as electric motors, lamps and heaters are less susceptible to damage from electromagnetic energy due to simpler designs and the absence of sensitive electronic components. Devices such as cell phones and hand-held radios with small antennas may also be less affected, especially if they are not connected to electrical sources during the EMP event. However, this also depends on the specific design and shielding of the device. In general, the effects of an EMP event can vary widely depending on the circumstances, but understanding the principles of susceptibility can help prepare for such an event.

#### CONCLUSIONS

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. CBRN threats to our country of great importance are related to the conflict in Ukraine. The study of nuclear and chemical hazards is necessary to generate information on the risks to the population and infrastructure not only on the territory of a country, but also on transboundary pollution. Nuclear war is the most threatening scenario in this context. The conflict in Ukraine has renewed attention to the possibility of nuclear war.

The threats and risks of nuclear explosions should not be ignored or glossed over. The software products used can be used in the prediction of the consequences of nuclear explosions at previously scouted targets. The article demonstrates the application of the proposed software platforms in the early warning system for the use of nuclear weapons after clearly defined factors (meteorological and nuclear blast parameters) and targets. In the civil defence line of thinking, the sole purpose is to consider what-if scenarios and focus on possible impacts on populations and societies.

#### 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] Dolchinkov, N. T., Nuclear weapons in NATO, International scientific journal: Science. Business. Society 4/2018, ISSN 2367-8380, pp. 181-184.
- [2] Маринов, А., Р., Анализ ефективността на симулатори и симулационни системи за обучение по тактическа подготовка, Годишник на ВА, С, 2012, стр. 18-28.
- [3] Horowitz, M.C., Artificial Intelligence, International Competition, and the Balance of Power, Texas National Security Review, Vol.1, Issue3, 2018.
- [4] Пъдарев, Н.И., Софтуерни инструменти за оценка на риска при използване на радиологично разпръскващо устройство, Годишник на НВУ 2019 част II, с. 79- 87, ВТ, 2019.
- [5] Димитров, Б. Управление на системата за ядрено, химическо и биологическо разузнаване. II International Scientific Conference Confsec 2018, pp. 122-124.
- [6] Dolchinkov, N. T., History and development of nuclear weapons, International scientific journal: Security@future 1/2018, pp. 32-35.
- [7] Николов Н. Х., Проблеми свързани със защитата на населението и териториите от поразяващите фактори на новите ОМУ, Сборник доклади от Научна конференция „Актуални проблеми на сигурността”, том 6, НВУ, 2019, с. 43-49.
- [8] Николов, Н. Х., Влиянието на оръжията за масово унищожение върху факторите на средата за сигурност. НВУ „В. Левски”, 2018, том 5, стр. 86, ISSN 2367-7465
- [9] Dolchinkov N., State of nuclear weapon in the world today, International scientific journal: Security@future 1/2019, ISSN 2535-0668 pp. 22-24
- [10] Hanfling, D., etc.. The right planning now will save countless lives after a nuclear attack, Bulletin of the Atomic Scientists, 2017, 73:4, 220-225, DOI: 10.1080/00963402.2017.1338005
- [11] Wellerstein, A. NUKEMAP. Available from [https://nuclearsecrecy.com/nukemap] (accessed on 20 Feb. 2024)
- [12] Пъдарев, Н., Прогнозиране на опасностите за населението и инфраструктурата при ядрени, радиологични и химически опасни събития чрез симулационни модели, Монография, Изд. НВУ, ВТ, 2021, ISBN ISBN 978-954-753-330-1
- [13] Ramana, M. V., Effects of nuclear weapons (IPPNW Global Health Watch Report no. 3.) Cambridge, MA: International Physicians for the Prevention of Nuclear War, 1999.
- [14] Dolchinkov, N. T., State of the population disclosure systems in the changing radiation situation in Bulgaria, Vide. Tehnologija. Resursi - Environment, Technology, Resources, 2019, 1, pp. 54-58

# Effect of precipitation and contamination origin on the efficiency of pinacolyl alcohol identification in concrete debris

**Jakub Pavlik**

Nuclear, Biological and Chemical Defence Institute  
University of Defence  
Vyskov, Czech Republic  
jakub.pavlik@unob.cz

**Tomas Rozsypal**

Nuclear, Biological and Chemical Defence Institute  
University of Defence  
Vyskov, Czech Republic  
tomas.rozsypal@unob.cz

**Abstract.** Chemical warfare agents (CWAs) pose a significant threat to people and the environment. Nowadays, the war fights take place mostly in urban areas. Here, chemical weapons contaminate materials of different properties, and the behavior of the parent contaminant may vary. Concrete has an alkaline pH and rapidly decomposes chemical warfare agents. The study deals with the analysis of potentially contaminated concrete samples taken from the site of the alleged use of nerve CWA soman (GD, pinacolyl methylphosphonofluoridate) using gas chromatography. The final degradation product of soman alkaline hydrolysis – pinacolyl alcohol (3,3-dimethylbutan-2-ol) – was chosen as the analyte. The method for the preparation of the concrete samples included organic solvent extraction of the contaminant, in which two organic solvents with different polarity, namely acetone and ethyl acetate, were used separately for comparison. The applicability of the method; the extraction efficiency from concrete debris at given time intervals from the time of contamination to the start of extraction; the effect of moisture addition before and after contamination; and the effect of the extractant used were studied. The possibilities of wipe sampling of the concrete surface in case of point and area contamination with pinacolyl alcohol were also monitored. The precision of the quantitative analysis was expressed by measuring the standard deviation and was worse in the case of ethyl acetate. The highest recovery values were observed with extraction from dry concrete, followed by concrete moistened after contamination. In the case of area contamination, a lower efficiency of surface wipe sampling was found. The results are particularly useful in the field analysis of samples after the use of chemical weapons.

**Keywords:** Chemical weapons, field analysis, gas chromatography, nerve agents, soman, wipe sampling.

## I. INTRODUCTION

In today's world, conducting military operations in urban areas is becoming much more common than in the past, and in future conflicts this form of operation is inevitable [1]. Chemical warfare agents (CWAs) still pose a significant threat to people and the environment, and the knowledge of the collection and subsequent preparation of a sample plays an important role for the identification of a CWAs by commonly used gas chromatography and mass spectrometry (GC/MS) in military deployable laboratories [2].

Nerve agent soman, (GD; pinacolyl methylphosphonofluoridate) belonging among the Schedule 1 substances of the Chemical Weapons Convention, possesses several noteworthy properties. Its toxicity characteristics include a low lethal dose to humans (LD<sub>50</sub>), which stands at 0.35 grams [3], [4]. Additionally, GD is resistant to antidotes due to its rapid ageing in the body. Furthermore, it demonstrates relatively high persistence in the environment, with a vapor pressure (VP) of 53.3 Pa at 25°C [4]. GD is colorless to brown liquid that is relatively odorless in its pure state, but impurities may cause a fruity or camphor odor [4]. It is slightly soluble in water (2.1 %) and very soluble in fats [4] and can therefore easily penetrate the human skin [5].

Hydrolysis of GD is a common process of environmental degradation. It occurs across a range of pH environments, including neutral, acidic, and basic conditions. However, alkaline hydrolysis stands out as the most efficient mechanism [5]. Consequently, when decontaminating surfaces contaminated with GD, alkaline hydrolysis serves as the primary method [5]. The intermediate product of GD hydrolysis is pinacolyl methylphosphonic acid, which is further and much more slowly hydrolysed to the final hydrolysis products, methylphosphonic acid and pinacolyl alcohol (PA), (3,3-dimethylbutan-2-ol) [5]. The reaction takes up to 60 h at pH 6 and 25 °C. In diluted solutions, GD is hydrolysed within 1.8 min at pH 10.8 [6] and the reaction rate

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8190>

© 2024 Jakub Pavlik, Tomas Rozsypal. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

increases with temperature [5]. Degradation products can also be used as a longer-term indicator of the use of GD in the environment and may play a key role in the identification of the parent agent [5]. Moreover, PA does not need to be derivatised for identification by gas chromatography, thus providing a good indicator of past GD present [7].

Concrete is an important substrate due to its wide use in construction and constitutes a significant portion of debris generated by a potential attack [8]. Concrete is characterised, among other properties, by porosity, alkaline pH  $\sim 12$  [9] and permeability to liquids, depending on the type of concrete [10]. From this we can conclude that contamination of concrete with liquid GD leads to its penetration into the matrix and subsequent efficient and rapid alkaline hydrolysis to methylphosphonic acid and PA due to high pH.

Identification of Chemical Warfare Agents and their fate in concrete has been the subject of extensive research by various authors. These studies primarily focus on several specific agents, including sulfur mustard [11], [12], sarin [13], tabun [14], adamsite [15] or VX [8]. In the context of preparing samples contaminated with chemical substances related to the Chemical Weapons Convention for analysis "Recommended operating procedures for analysis in the verification of chemical disarmament" (Blue Book) - have been developed by the Finnish Institute for Verification of Compliance with the Chemical Weapons Convention (VERIFIN) including a recommended procedure for the preparation of both concrete. These procedures are validated in OPCW testing and are widely used by laboratories worldwide [16]. The procedure for briefly starts with a small amount of concrete sample (1-5 g), which is homogenized by crushing if necessary. Extraction with an organic solvent (e.g. acetone or dichloromethane), water and 1M HCl are then used in sequence. Finally, the three fractions of the samples are further separated, some of them evaporated to dryness and derivatised with the appropriate reagents if necessary [17]. However, this procedure is time-consuming, difficult to implement and does not suit field conditions. Also, it's worth noting that the influence of meteorological conditions or contamination origin was not thoroughly considered or studied in these investigations.

The aim of the study is to optimize the developed sample preparation method applicable in military deployable laboratories, observe the extraction efficiency of PA from 2 types of concrete debris – lost formwork and steel fibre reinforced concrete (SFRC) at specified periods from the time of contamination to the start of extraction, the effect of moisture addition before and after contamination and the effect of the used extractant – acetone (Acon) and ethyl acetate (Etac). There were also monitored the possibilities of wipe sampling of the concrete surface in case of point and area contamination with PA, simulating accidental spillage of liquid or dispersion from a chemical munition.

## II. MATERIALS AND METHODS

### A. Reagents and Material

The stock solution (concentration  $7.56 \text{ mg}\cdot\text{mL}^{-1}$ ) used for concrete contamination was prepared from 99%

pinacolyl alcohol (VOZ Zemienské Kostol'any, Slovakia) dissolved in 99.8% dichloromethane (Merck, Darmstadt, Germany). Ethyl acetate 99.7 % (Sigma-Aldrich, Steinheim, Germany) and 99.5% acetone (Chromservis, Praha-Petrovice, Czech Republic) were used as solvents for the extraction of PA.

The concrete samples consisted of two different types of concrete. The first type was a lost formwork made of plain and lightweight concrete (DITON s.r.o., Stritez, Czech Republic), which represented a less homogeneous and more porous concrete sample. [18]. The second type was cut steel fibre reinforced concrete blocks (dimensions  $3.5 \text{ cm} \times 3.5 \text{ cm} \times 3.5 \text{ cm}$ , weight 75–85 g) with compressive strength class C30/37 and exposure class XC4 – cyclical wetting and drying [19] this type is used in applications where steel wires completely replace standard reinforcement or are used in combination. A typical example of its use is polished industrial floors [20]. This type of concrete, on the other hand, represented a more homogeneous and less porous concrete sample.

The extracts were analysed by a gas chromatograph with flame ionization detector GC/FID Trace 1310 (Thermo Fisher Scientific Inc., USA). The column was TG-5MS, dimensions  $30 \text{ m} \times 0.32 \text{ mm} \times 0.50 \text{ mm}$ . The column temperature was set so that the temperature was  $80 \text{ }^\circ\text{C}$  for 2 min, then with a temperature gradient of  $20 \text{ }^\circ\text{C} \cdot \text{min}^{-1}$  the temperature was increased to  $280 \text{ }^\circ\text{C}$  and then left at this temperature for another 2 min. The total duration of the method was 15 minutes. The injection port temperature was set at  $250 \text{ }^\circ\text{C}$  and the injection was performed in split mode with a ratio of 1:13. A constant flow of  $1.5 \text{ mL} \cdot \text{min}^{-1}$  carrier gas (helium) was applied to the column. The flame ionization detector was used for data acquisition throughout the method, the detector temperature was  $280 \text{ }^\circ\text{C}$ . The flame generation gases were set at flow rates of  $350 \text{ mL} \cdot \text{min}^{-1}$  (air) and  $40 \text{ mL} \cdot \text{min}^{-1}$  (hydrogen). In addition, an additional inert gas (make-up gas) was injected into the system at a flow rate of  $30 \text{ mL} \cdot \text{min}^{-1}$  (nitrogen). A sample volume of  $1 \text{ } \mu\text{L}$  was injected into the instrument using a TriPlus RSH autosampler (Thermo Fisher Scientific Inc., USA) using the "hot needle" method.

The following instruments were used for sample preparation: ultrasonic bath Sonorex Super RK 106 (Bandelin), laboratory centrifuge Janetzki T5 (LAB system), analytical balance (Mettler Toledo), automatic pipettes (maximum volume  $200 \text{ } \mu\text{L}$ ,  $1 \text{ mL}$  and  $5 \text{ mL}$ , Transferpette), laboratory refrigerator and laboratory dryer. Other laboratory equipment included DURAN wide-mouth laboratory bottles with lids ( $100 \text{ mL}$  volume, Fisherbrand), low glass beakers ( $150 \text{ mL}$  volume), hour glass ( $70 \text{ mm}$  diameter), petri dish ( $60 \text{ mm}$  diameter) hammer, tweezers, screw, desiccator, cap vials ( $5 \text{ mL}$  and  $2 \text{ mL}$  volume).

### B. Procedures for monitoring the effect of precipitation

When monitoring the effect of precipitation on extraction efficiency, 3 cases were studied: moisture addition to the sample before contamination, moisture addition to the sample after contamination and dried sample. These cases were monitored for both types of concrete.



### 1) *Lost formwork samples*

The preparation of lost formwork samples involved breaking the lost formwork with a hammer into concrete fragments weighing approximately 10-30 g, which were then dried in a laboratory dryer (10 min, 100 °C) and then cooled to laboratory temperature in a desiccator.

The moisture addition before contamination involved moistening the concrete fragments evenly with water equal to 3 % of the weight of the concrete fragment before contamination. After 1 minute the fragments were evenly contaminated with 200 µL of 7.56 mg·mL<sup>-1</sup> PA solution.

The moisture addition after contamination involved even contamination of the fragments with 200 µL of 7.56 mg·mL<sup>-1</sup> PA solution. After a period of 1 hour, the fragments were evenly moistened with water equal to 3 % of the weight of the concrete fragment.

Contamination of the dried concrete fragments involved even contamination of the fragments with 200 µL of 7.56 mg · mL<sup>-1</sup> PA.

The samples thus prepared for the 3 different experiments were then left on petri dishes at laboratory conditions for a specified period. Then the samples were transferred to 100 ml wide-mouth Fisherbrand DURAN laboratory bottles, 30 ml of Acon or Etac was applied directly in each bottle and the bottles were tightly capped. These bottles were then sonified in an ultrasonic bath for 30 minutes. After the extraction, 4 mL of the solution was transferred from the bottles into 5 mL vials and centrifuged for 5 minutes. Finally, 1 mL of the cleared solution was transferred into GC vials which were sealed and prepared for the analysis.

### 2) *SFRC samples*

The preparation of SFRC samples involved drying in a laboratory dryer (10 min, 100 °C) and then cooled to laboratory temperature in a desiccator. Contamination of the SFRC blocks took place only on one side of the block (average area - 10 cm<sup>2</sup>).

The moisture addition before contamination involved moistening with 20 µL of water per cm<sup>2</sup> of contamination area. The water droplets were then spread evenly over the area to be contaminated using tweezers, as this type of concrete did not properly absorb liquid. After 1 minute the blocks were evenly contaminated with 100 µL of 7.56 mg·mL<sup>-1</sup> PA solution.

The moisture addition after contamination involved even contamination of the blocks with 100 µL of 7.56 mg · mL<sup>-1</sup> PA solution. After a period of 1 hour, the contamination area was moistened with 20 µL of water per cm<sup>2</sup>. The water droplets were then spread evenly over the area to be contaminated using tweezers.

Contamination of the dried concrete samples involved even contamination of the one side of the SFRC blocks with 100 µL of 7.56 mg·mL<sup>-1</sup> PA solution.

The samples thus prepared for the 3 different experiments were then left on petri dishes at laboratory conditions for a specified period. Then the samples were transferred to 150 mL beakers, 10 mL of Acon or Etac was applied at the bottom of each beaker and covered with a petri dish. These beakers were then sonified in an

ultrasonic bath for 30 minutes. After the extraction, 2 mL of the solution was transferred and centrifuged for 5 minutes. Finally, 0.6 mL of the cleared solution was transferred into GC vials for analysis.

### *C. Procedures for monitoring the effect of contamination origin*

The effect of contamination origin on the extraction efficiency of PA was also monitored for both types of concrete. In this experiment, 100 µL of 7.56 mg·mL<sup>-1</sup> PA solution for lost formwork samples or 50 µL of 7.56 mg·mL<sup>-1</sup> PA solution for SFRC samples was applied, depending on the experiment, either to a single point on the sample or the contaminant was applied evenly to cover the largest area. Then, after a specified period, a circular motion was made to wipe using tweezers and cellulose soaked in Acon or Etac. The cellulose was then placed in a 100 mL wide-mouth Fisherbrand DURAN laboratory bottle with 30 mL of Acon or Etac and sonified in an ultrasonic bath for 30 minutes. After the extraction, 4 mL of the solution were centrifuged, and the liquid extract was analyzed.

## III. RESULTS AND DISCUSSION

The data processing was carried out based on the determination of 3 calibration series of PA solutions in dichloromethane, a linear calibration curve with a coefficient of determination  $R^2 = 0.9991$  was established, which was used to calculate the mass concentrations of PA in the sample. The concentration of the stock solution of PA (7.56 mg·ml<sup>-1</sup>) was chosen so that the maximum theoretical recovery was within the calibration curve, where the upper point is equal to 50 µg·ml<sup>-1</sup>. The mass concentration values were converted to the observed extraction efficiency of PA ( $E_{obs}$ ), i.e. the percentage theoretical recovery of PA throughout the sample preparation. The arithmetic mean of these efficiencies and its standard deviation were calculated from the individual values of the  $E_{obs}$  of the sample replicates. The magnitude of the  $E_{obs}$  served as a comparative criterion for the different procedures in this work.

A. The effect of precipitation

In this experiment, PA was applied to a) an already moistened concrete sample (moistened before), b) a concrete sample that was moistened 1 hour after contamination (moistened after) and c) a dried concrete sample (dried sample) to compare the resulting extraction efficiency. These cases simulate influence of precipitation and moisture before and after contamination on extraction efficiency and compare extraction efficiency with

Each experiment of concrete lost formwork samples was measured 3 times, in total 174 samples were used, to obtain statistical data and standard deviations for the precision of analysis. The mean values of the detected  $E_{obs}$  are shown in the graphs for Acon (Fig. 1.) and Etac (Fig.2.) separately.

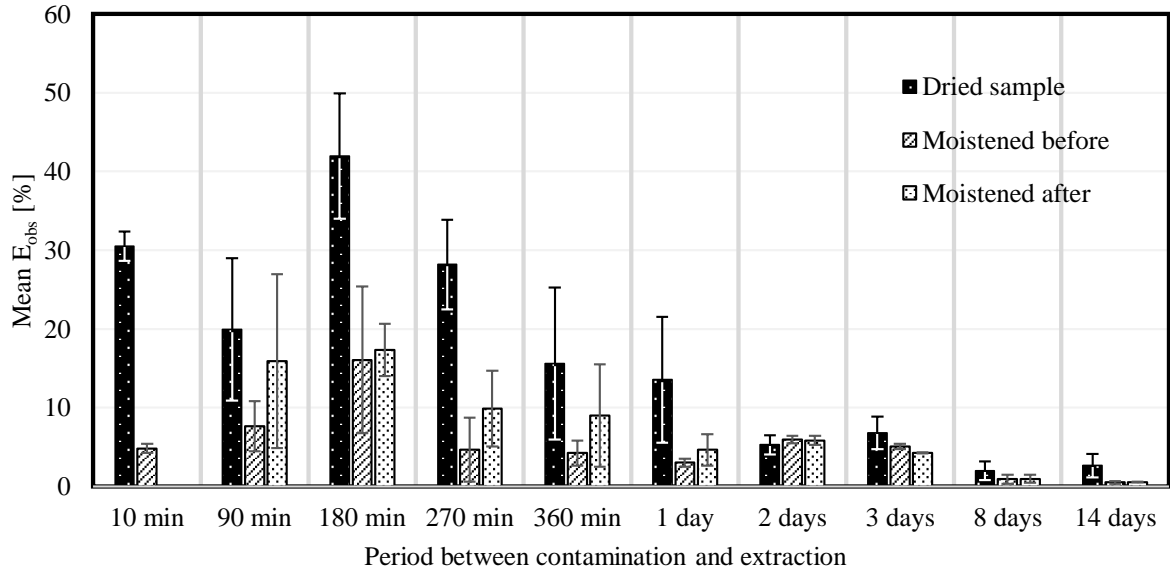


Fig. 1. The mean values of the observed extraction efficiency of pinacolyl alcohol ( $E_{obs}$ ) at periods using acetone as extractant of concrete lost formwork samples.

contaminated dried samples. The effect of the period from contamination to extraction on  $E_{obs}$  was also monitored. A total of 10 periods (10, 90, 270, 360 minutes and 1, 2, 3, 8, 14 days) were tested to monitor the decrease in concentration within a short time after the contamination and to emphasize the importance of early intervention. The suitability of Acon and Etac used for extraction and both types of concrete samples were also tested and compared.

1) Lost formwork samples

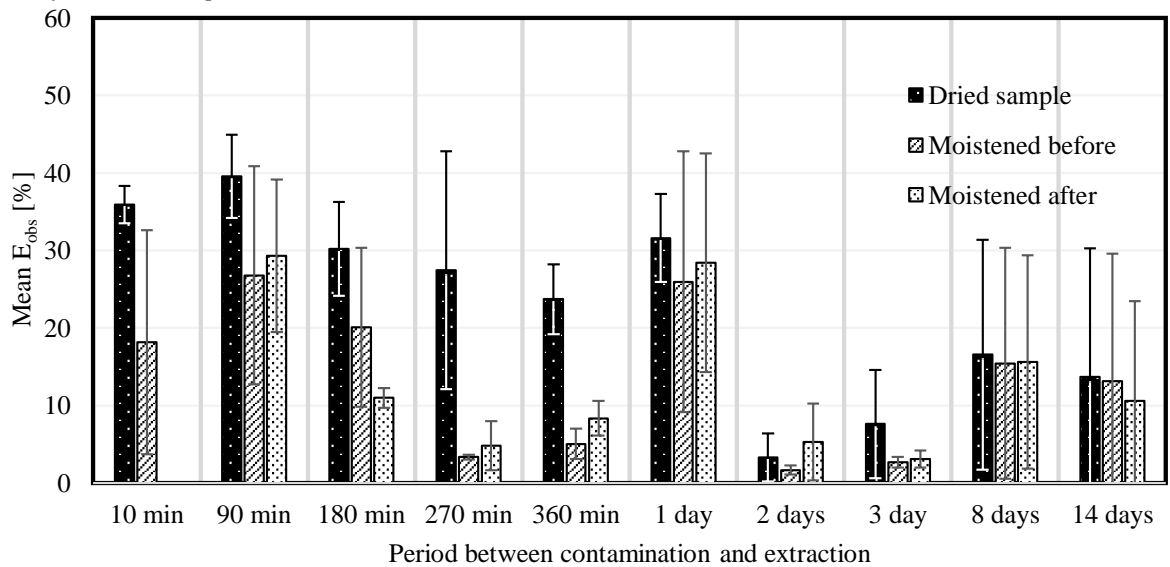


Fig. 2. The mean values of the observed extraction efficiency of pinacolyl alcohol ( $E_{obs}$ ) at periods using ethyl acetate as extractant of concrete lost formwork samples.

High deviations caused by the different structure of lost formwork fragments were observed. The different structure may have caused volatile PA to evaporate, become trapped deeper in the fragment structure or desorbed with added water. We also observed that  $E_{obs}$  is highest in the dried samples where the extraction was not disturbed by the presence of water and lowest when the samples are moistened before contamination where PA could not be absorbed into the concrete to the same extent as in other experiments due to moisture. Etac as an extraction reagent showed higher  $E_{obs}$  overall, but also had higher standard deviations than Acon for cases of moistened samples. Acon as an extraction reagent had lower  $E_{obs}$  for moistened samples compared to dried samples.

Each experiment of SFRC samples was measured 2 times, in total 116 SFRC blocks were used as samples. The mean values of the detected  $E_{obs}$  are shown in the graphs for Acon (Fig. 3.) and Etac (Fig. 4.) separately.

SFRC samples provided overall lower  $E_{obs}$  compared to lost formwork samples due to their low porosity and liquid absorption, but compared to the results from the lost formwork, the SFRC samples are more consistent in decreasing  $E_{obs}$  over periods due to their more homogenous structure. Etac again showed significantly higher  $E_{obs}$  in all 3 cases than Acon. Moistening the samples produced a similar effect to that of lost formwork samples.

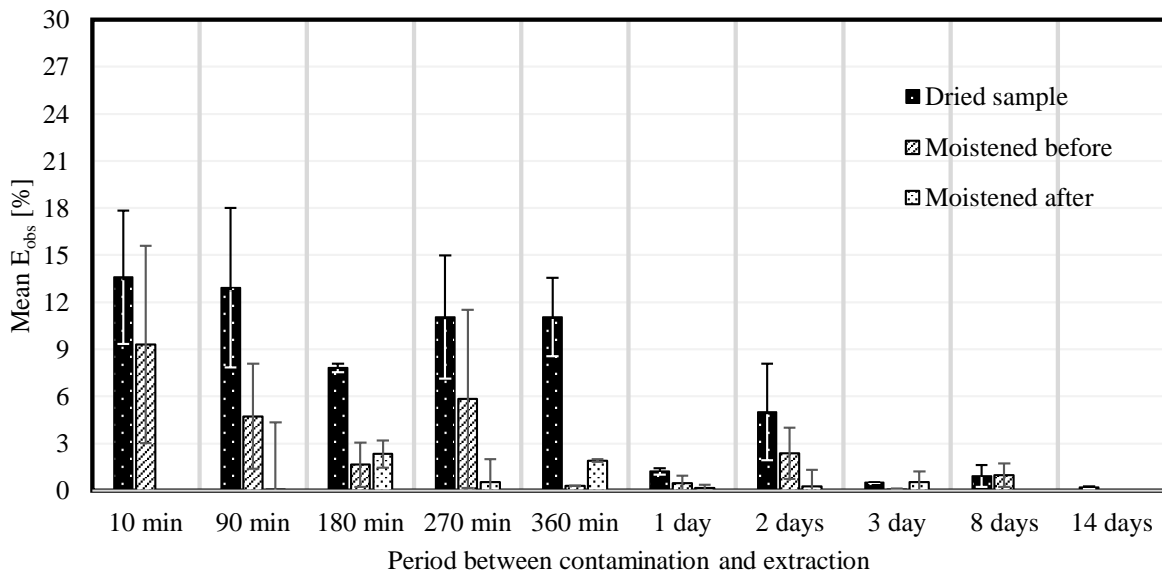


Fig. 3. The mean values of the observed extraction efficiency of pinacolyl alcohol ( $E_{obs}$ ) at periods using acetone as extractant of steel fibre reinforced concrete samples.

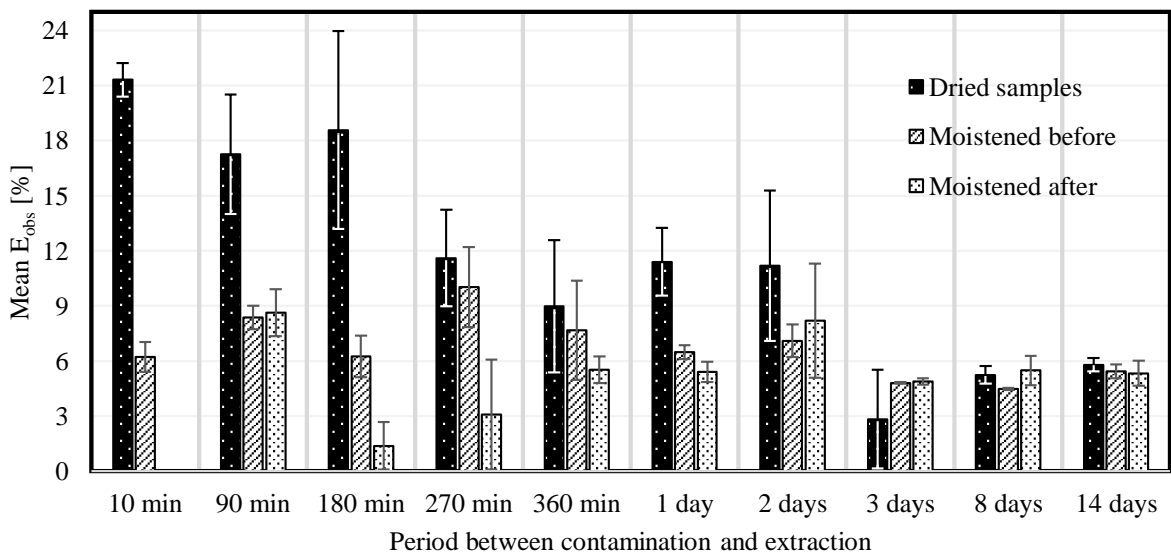


Fig. 4. The mean values of the observed extraction efficiency of pinacolyl alcohol ( $E_{obs}$ ) at periods using ethyl acetate as extractant of steel fibre reinforced concrete samples.

SFRC samples

For SFRC, the lowest results were obtained when analyzing samples that were wetted after contamination. The low porosity of the material causes retention of the contaminant (PA) on the surface. The fate of PA in this scenario is evaporation. When water is added, it washes and dilutes the contaminant from the surface reducing the final sampling recovery. In the case of lost formwork, the porosity is considerably higher. Adding water after contamination does not significantly affect recovery compared to samples moistened before contamination with PA. It can be evaluated that meteorological influences differ for concrete samples based on their technical properties. In summary, understanding these variations is crucial for effective sampling but also decontamination strategies in different concrete scenarios.

### B. The effect of contamination origin

In this experiment, the effect of area and point contamination of concrete on extraction efficiency was studied using 2 cases that simulated dispersion of CWA by chemical munitions or other means (area contamination) and accidental spillage of liquid on concrete (point contamination). In the case of area contamination, sample was evenly contaminated with PA and in the case of point contamination, the contaminant was applied to a single point on the concrete sample and after 10 minutes, a wipe was taken using cellulose moistened in used solvent. In this experiment, Acon and Etac solvents were again used as extraction reagents and both types of concretes were used for comparison.

#### 1) Lost formwork samples

Each experiment was measured 5 times to obtain statistical data. The results from the measurement of the

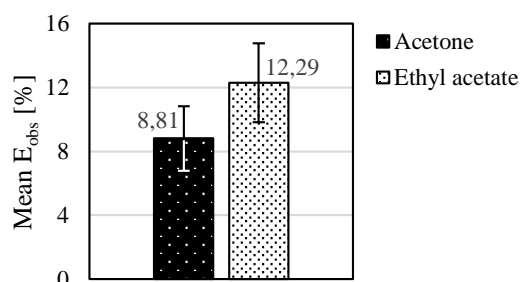


Fig. 5. The mean values of the observed extraction efficiency of pinacolyl alcohol ( $E_{obs}$ ) for acetone and ethyl acetate as extractant for point contamination of lost concrete

point contamination and area contamination are divided

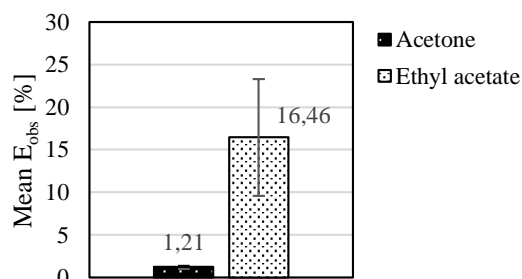


Fig. 7. The mean values of the observed extraction efficiency of pinacolyl alcohol ( $E_{obs}$ ) for acetone and ethyl acetate as extractant for point contamination of steel fibre reinforced samples

into 2 graphs (Fig. 5., Fig. 6.).  $E_{obs}$  of point contamination were generally higher than in the case of area contamination due to a better penetration of PA into the structure of the concrete sample. Also, the  $E_{obs}$  for Etac was higher than for Acon.

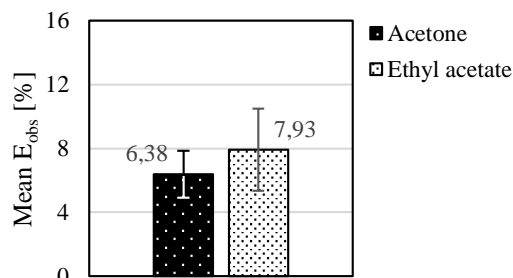


Fig. 6. The mean values of the observed extraction efficiency of pinacolyl alcohol ( $E_{obs}$ ) for acetone and ethyl acetate as extractant for area contamination of lost concrete

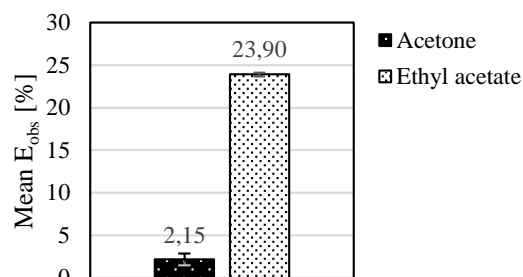


Fig. 8. The mean values of the observed extraction efficiency of pinacolyl alcohol ( $E_{obs}$ ) for acetone and ethyl acetate as extractant for area contamination of steel fibre reinforced samples

#### 2) SFRC samples

Each experiment was measured 3 times and the results from the measurement of the point contamination and area contamination are also divided into 2 graphs (Fig. 7., Fig. 8.).

Different results were observed for the SFRC samples than for the lost formwork samples.  $E_{obs}$  in the case of point contamination were overall lower than in the case of area contamination due to high evaporation and inability to absorb in less porous material. Etac gave us significantly higher  $E_{obs}$  than Acon, which gave  $E_{obs}$  within 3 %.

## CONCLUSIONS

From the results obtained, we can conclude that precipitation, the origin of contamination, the type of concrete and the extraction reagent have a significant effect on the resulting extraction efficiency of PA.

The highest extraction efficiency values were observed with extraction from dry concrete, followed by concrete moistened after contamination. Acetone had an overall lower extraction efficiency than ethyl acetate and a markedly lower extraction efficiency when the concrete sample was moistened than in case of dried concrete but showed smaller standard deviations. Ethyl acetate had a higher extraction efficiency compared to acetone but is not

very suitable for quantitative analysis due to the standard deviations obtained. Ethyl acetate also produced additional unwanted peaks on the chromatograms which could interfere with the analysis. Therefore, for identification purposes, acetone is a better extraction reagent.

In the case of area contamination, a lower efficiency of surface wipe sampling was found when using samples from porous lost formwork samples, but a higher efficiency of surface wipe sampling was observed when using less porous SFRC samples.

The work is limited by testing in laboratory conditions that do not fully reflect real conditions. Temperature is chosen constant, rainfall is simulated by the addition of water, the effect of wind is omitted. Nevertheless, the results allow us to make assumptions for development in a real environment.

For comparison, the method presented in the Blue Book is more time-consuming and more difficult, which is not suitable for field conditions. The Blue Book also assumes smaller sample volumes and possible homogenization by crushing, which is only possible if a laboratory crusher is used. Homogenization leads to contamination of the instruments used and to loss of contaminant due to evaporation. In addition, due to the high porosity of concrete, wipe sampling appears to be a less effective sampling method and may not lead to successful identification.

In summary, the developed method is a simple but applicable method for the identification of contaminants in concrete samples. The results show that understanding meteorological factors, properties of concrete and their impact on extraction efficiency is crucial for effective contaminant identification on concrete samples and decontamination strategies. Precipitation reduces the analytical recovery, as does a more homogeneous type of concrete. Further research should include the use of the CWAs themselves and other degradation products as contaminants to validate the method.

#### ACKNOWLEDGMENTS

The work was financed from the resources of the Ministry of Education, Youth and Sports of the Czech Republic within the framework of the student grant competition project "Sampling and analysis of urban debris as evidence samples after the use of chemical weapons".

#### REFERENCES

- [1] A. Vautravers, "Military operations in urban areas," *International Review of the Red Cross*, vol. 92, no. 878, pp. 437–452, Jun. 2010, doi: <https://doi.org/10.1017/s1816383110000366>.
- [2] J. T. Kelly, A. Qualley, G. T. Hughes, M. H. Rubenstein, T. A. Malloy, and T. Piatkowski, "Improving Quantification of tabun, sarin, soman, cyclosarin, and sulfur mustard by focusing agents: A field portable gas chromatography-mass spectrometry study," *Journal of Chromatography A*, vol. 1636, p. 461784, Jan. 2021, doi: <https://doi.org/10.1016/j.chroma.2020.461784>.
- [3] "Schedule 1," *OPCW*. <https://www.opcw.org/chemical-weapons-convention/annexes/annex-chemicals/schedule-1>
- [4] D. Hank Ellison, *Handbook of Chemical and Biological Warfare Agents, Volume 1*. 2022. doi: <https://doi.org/10.4324/9781003230571>.
- [5] I. S. Che Sulaiman *et al.*, "A review on analysis methods for nerve agent hydrolysis products," *Forensic Toxicology*, vol. 38, no. 2, pp. 297–313, Dec. 2019, doi: <https://doi.org/10.1007/s11419-019-00513-x>.
- [6] S. Popiel and M. Sankowska, "Determination of chemical warfare agents and related compounds in environmental samples by solid-phase microextraction with gas chromatography," *Journal of Chromatography A*, vol. 1218, no. 47, pp. 8457–8479, Nov. 2011, doi: <https://doi.org/10.1016/j.chroma.2011.09.066>.
- [7] T. Rozsypal, Kristyna Zitova, and Ludmila Mravcova, "Overcoming the BSTFA: Study on Trimethylsilylation Derivatization Procedures for Chemical Weapons Convention-Related Alcohols in Field Analysis," *Analytical Letters*, pp. 1–17, Nov. 2023, doi: <https://doi.org/10.1080/00032719.2023.2281587>.
- [8] J. W. Williams *et al.*, "Degradation Kinetics of VX on Concrete by Secondary Ion Mass Spectrometry," *Langmuir*, vol. 21, no. 6, pp. 2386–2390, Feb. 2005, doi: <https://doi.org/10.1021/la047933j>.
- [9] Y. Sumra, S. Payam, and I. Zainah, "The pH of Cement-based Materials: A Review," *Journal of Wuhan University of Technology-Mater. Sci. Ed.*, vol. 35, no. 5, pp. 908–924, Oct. 2020, doi: <https://doi.org/10.1007/s11595-020-2337-y>.
- [10] A. M. Neville, *Properties of concrete*. Harlow Pearson Education, 2012.
- [11] C. A. S. Brevett, K. B. Sumpter, G. W. Wagner, and J. S. Rice, "Degradation of the blister agent sulfur mustard, bis(2-chloroethyl) sulfide, on concrete," *Journal of Hazardous Materials*, vol. 140, no. 1–2, pp. 353–360, Feb. 2007, doi: <https://doi.org/10.1016/j.jhazmat.2006.09.067>.
- [12] H. Jung and S. Choi, "Behavior of sulfur mustard in sand, concrete, and asphalt matrices: Evaporation, degradation, and decontamination," *Journal of Environmental Science And Health, Part A*, vol. 52, no. 12, pp. 1121–1125, Jul. 2017, doi: <https://doi.org/10.1080/10934529.2017.1342498>.
- [13] C. J. O'Brien, J. A. Greathouse, and C. M. Tenney, "Dissociation of Sarin on a Cement Analogue Surface: Effects of Humidity and Confined Geometry," *The Journal of Physical Chemistry C*, vol. 120, no. 49, pp. 28100–28109, Dec. 2016, doi: <https://doi.org/10.1021/acs.jpcc.6b10046>.
- [14] H. Jung, J. Lee, H. Park, and J. A. Seo, "Fate of Nerve Agent Tabun in Concrete and Soil: Evaporation and Decontamination," *Environmental Engineering Science*, vol. 36, no. 6, pp. 650–655, Jun. 2019, doi: <https://doi.org/10.1089/ees.2018.0535>.
- [15] T. Rozsypal, "Use of aliphatic thiols for on-site derivatization and gas chromatographic identification of Adamsite," *Journal of The Serbian Chemical Society*, vol. 88, no. 6, pp. 639–652, Jan. 2023, doi: <https://doi.org/10.2298/jsc221207025r>.
- [16] "Blue Book | VERIFIN | University of Helsinki," [www.helsinki.fi](http://www.helsinki.fi). <https://www.helsinki.fi/en/verifin/about-verifin/blue-book>
- [17] M. L. Kuitunen and N. Hamzah, "Concrete samples" in P. Vanninen (ed.) *Recommended operating procedures for analysis in the verification of chemical disarmament, 2023 Edition*, University of Helsinki, Finland, 2023, pp. 335–342. <http://www.helsinki.fi/verifin/bluebook>
- [18] Precast concrete products – Normal weight and lightweight concrete shuttering, EN 15435, 2008.
- [19] Concrete – Specification, performance, production and conformity, EN 206+A2, 2013
- [20] T. Błaszczyszki and M. Przybylska-Fałek, "Steel Fibre Reinforced Concrete as a Structural Material," *Procedia Engineering*, vol. 122, pp. 282–289, 2015, doi: <https://doi.org/10.1016/j.proeng.2015.10.037>.

# *Effectiveness of Electronic Governance in Crisis Management*

**Irena Peteva**

*National Security Department  
University of Library Studies and  
Information Technologies  
Sofia, Bulgaria  
i.peteva@unibit.bg*

**Ivanka Pavlova**

*Information and Communication  
Technologies Department  
University of Library Studies and  
Information Technologies  
Sofia, Bulgaria  
i.pavlova@unibit.bg*

**Daniela Pavlova**

*Computer Science Department  
University of Library Studies and  
Information Technologies  
Sofia, Bulgaria  
d.pavlova@unibit.bg*

**Abstract.** The research focuses on the role of electronic governance (e-Governance) in crisis management, highlighting the COVID-19 pandemic. Through a literature review and case studies analysis from various countries, including data on Bulgaria, this article explores how technologies support effective crisis management and offers ways to optimize electronic solutions in future crisis management strategies. The research methods include a qualitative analysis of data from publicly available sources, government reports, academic articles, and statistical data to identify successful practices and challenges in implementing electronic governance across different sectors during crises. The results show that Bulgaria has made significant progress in adapting and adopting electronic governance in response to the pandemic, highlighting the importance of technology in maintaining administrative functionality during crisis periods. The specific example of Chile, along with the Bulgarian experience in managing the pandemic, demonstrates the potential of technological solutions. The conclusions emphasize the need for developing flexible, scalable, and secure technological solutions for electronic governance, focusing on improving digital skills and infrastructure. Electronic governance has been identified as a key tool for crisis management that should be integrated into strategic crisis management plans. Future efforts should be directed towards enhancing technological platforms and developing innovative solutions for the resilience and efficiency of societies in crisis conditions.

**Keywords:** *e-Governance, COVID-19, Crisis Management*

## I. INTRODUCTION

In today's world, where we often face various forms of crises, from natural disasters to global health threats, effective management of these situations is essential to maintain stability and safety in society. The focus of this research paper is on the analysis of the role of e-Governance during crises, with a specific emphasis on the

consequences of the COVID-19 pandemic. The article provides an objective view of how technology can support and improve the effectiveness of crisis management through an analysis of existing practices and successful examples.

With this scientific article, we aim to contribute to the enrichment of knowledge in the field of crisis management by providing analysis, recommendations and perspectives for the future. In the following sections, we will look at specific examples and aspects of e-Governance in times of crisis in order to highlight the importance and opportunities that technology provides in this context. In addition to reviewing international practices and successful examples, this analysis includes specific data on Bulgaria, illustrating the application of electronic governance in response to the COVID-19 crisis. Thus, by combining an international review and national analysis, this article offers a comprehensive perspective on the opportunities and challenges associated with the effectiveness of electronic governance during crises.

## II. MATERIALS AND METHODS

The study of the effectiveness of e-Governance in crisis situations is based on strategically selected qualitative methods and a variety of sources. The approach includes analysis of scientific articles, government reports, and specific case studies, with a focus on real data from Bulgaria to illustrate key observations and conclusions. This methodology allows us to assess the direct impact of the electronic governance on crisis management and to derive comprehensive recommendations for its future development and application. Few people think that the presence of e-Governance is especially important during a crisis. In addition to the fact that the crisis (be it

*Print ISSN 1691-5402*

*Online ISSN 2256-070X*

<https://doi.org/10.17770/etr2024vol4.8226>

© 2024 Irena Peteva, Ivanka Pavlova, Daniela Pavlova.

*Published by Rezekne Academy of Technologies.*

*This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)*

natural, financial, political, health or other) usually leads to a lower purchasing power of citizens, it almost always results in a sharp contraction of public spending, or, in other words - if we try to realize certain public policies – social, educational, etc., we will just have to be able to do it with less money. One of the main characteristics of e-Governance is that it saves money and optimizes processes, which is one of the prerequisites to consider that the role of e-Governance is particularly important in crises situations, and even to some extent a crisis is a catalyst for the development of e-Governance because otherwise there is no way to achieve the same effect with the available resources spent inefficiently [1].

A crisis can hit us in the most diverse ways – closing down productions, shrinking job positions, civil unrest, etc. In fact, in each of these situations e-Governance can play a certain positive role, as long as we are able to use it to its full potential. For example, when factories are closed or jobs are downsized, appropriate systems developed within e-Governance can assist us in finding work. At the same time, the companies or institutions where the layoffs are taking place will have to continue to function, and for this purpose the reduced staff should be able to perform the same amount of work, for which again electronic governance comes to the rescue. There is a certain objective logic in accelerating the pace of e-Governance penetration when the economic situation worsens, since in practice it is a kind of medicine against crises, but of course, it is by no means a panacea and cannot solve every specific situation. It is important that society realizes and accepts its key role in the reengineering of processes that invariably accompanies e-Governance, while transparency and publicity, which are also inherent in e-Governance, play an important role in calming public opinion, making the whole society complicit with what is happening [1].

Chile is one of the most disaster-prone countries because it lies on a “ring of fire” tectonic plate. The 8.8-magnitude earthquake that struck there in 2010 was the world's sixth largest since 1900. In the aftermath, the Chilean government took progressive steps toward establishing a tsunami early warning system. A network of pressure sensors has been installed near the main fault lines between Peru and Chile. The sensors detect the number of seismic events and the software estimates the magnitude and epicenter. An algorithm analyzes and interprets the data before passing it on to alert centers. Early warning messages are broadcast over the mobile phone network [2].

The importance of electronic governance significantly increases in crisis situations caused by natural disasters, health crises, or socio-economic changes, often aiding in maintaining social stability and the efficiency of public services. Especially during a crisis, when resources are limited, electronic governance offers opportunities for process optimization and cost savings. The example of Chile and the development of a tsunami early warning system following the 2010 earthquake illustrates how technological solutions can save lives and reduce economic losses. Thus, electronic governance not only facilitates the management of immediate crisis situations but also supports the long-term adaptation of societies to changing conditions, playing a key role in overcoming challenges and building more resilient socio-economic systems.

### III. RESULTS AND DISCUSSION

In the context of global crises, the effective and adaptive management becomes not only a challenge but also a crucial factor for survival and recovery. In this section, our research reveals how electronic governance emerges as an important tool in crisis management, with a special focus on the COVID-19 pandemic. We have examined the significance of technological innovations and digital integration in the context of crisis response, highlighting how the COVID-19 crisis has pointed out the need for accelerated development and application of electronic solutions in public administration. Additionally, we have analysed the role of electronic governance as a catalyst for socio-economic adaptation. The aim of this section is not only to provide an objective analysis of the observed phenomena but also to offer recommendations that can serve as a basis for formulating future strategies for electronic governance. The intention is to emphasize the potential of the electronic governance not only as a means to cope with current crises but also as a crucial element in strategic planning for sustainable and innovative management of society. Through this discussion, our aim is to contribute to the expansion of knowledge about electronic governance as a tool for sustainable and effective crisis management, offering recommendations that can improve its effectiveness in future emergencies.

The COVID-19 crisis has played a key role in accelerating business processes and promoting innovation in various fields. The pandemic has become a catalyst for changes that include not only adaptation to new realities, but also the adoption of technological transformations. The COVID-19 crisis, instead of being only a challenge, has become an opportunity for innovation and progress, with changes in business processes and the adoption of new technologies becoming inevitable for sustainability and development. The outbreak of the COVID-19 pandemic in early March 2020, followed by a lockdown, created new pressures from both institutions and citizens to deepen and accelerate e-Governance reforms to ensure continuity of work processes and the provision of public services. This has led several institutions that previously considered e-Governance to be a low-priority issue to express an increased interest in reforms to ensure their resilience to possible future crisis shocks [3].

The COVID-19 pandemic has caused serious challenges for administrations around the world, necessitating the need for innovative and effective management methods. According to the data in the reports [4], [5] of the United Nations study on the development of e-Governance during the period of the COVID-19 crisis (2020-2022), information and communication technologies (ICT) played a key role in supporting health and safety of people and in ensuring the functioning of economies and societies. The pandemic has highlighted the importance of e-Governance as a means of improving services to society and accelerating the achievement of sustainable development goals. E-Governance technologies have kept governments and citizens connected during the pandemic by sharing information and delivering services electronically. This has enabled governments to make rapid policy decisions based on real data and

analyses and to increase the capacity of local authorities for better coordination and service delivery. Governments shared information through their national portals, mobile apps and social networks. A review of the national portals of the 193 members of the United Nations reveals that governments have shown a high level of transparency in providing information related to the crisis. Some governments have shown great flexibility by developing dedicated COVID-19 portals and government apps, providing continuously up-to-date information and resources to combat the pandemic “Fig. 1”.

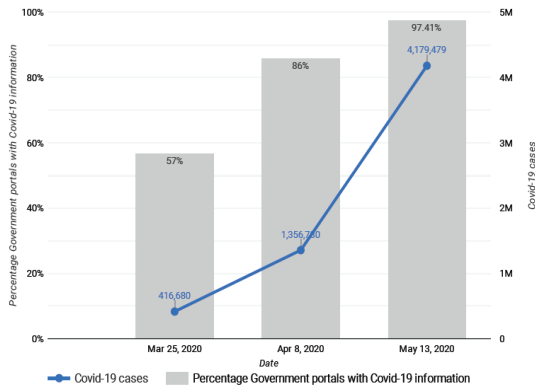


Fig. 1. Percentage of Government portals with COVID-19 information and world total confirmed COVID-19 cases [4] – [8].

A review of the national portals of 193 United Nations Member States showed that as of 25 March 2020, only 57 percent (110 countries) had provided any information on COVID-19. The percentage of countries providing such information and guidance reached approximately 86 percent (167 countries) as of April 8, 2020. Finally, as of May 13, almost 97.5 percent (188 countries) already had information about COVID-19 in their national portals [4].

Innovations, including the use of artificial intelligence, blockchain and robotics, have contributed to the fight against the pandemic and highlighted the need for effective, inclusive and accountable digital governance. In the future, strategies should focus on improving data protection and global digital inclusion by strengthening the political and technical capacities of public institutions. At the same time, challenges such as information security and disinformation require responsible and concerted efforts by governments.

The analysis of data from recent years in Bulgaria shows a significant increase in the number of joined administrations in 2020 and 2021 “Fig. 2”. This period is characterized by rapid adaptation to electronic solutions, which play a key role in maintaining the functionality of administrative systems during a crisis.

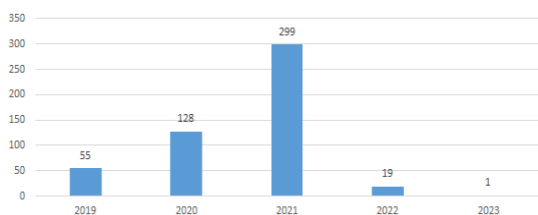


Fig. 2. Administrations that have joined the Single Model. The data is current as of 02/20/2024 [6].

The year 2021 stands out as a period with an extremely high number of developed electronic services “Fig 3”. This fact emphasizes the commitment to the improvement of electronic platforms and the provision of innovative solutions.

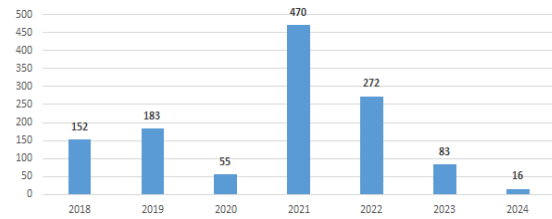


Fig. 3. Number of services developed under the Unified Model. The data is current as of 02/20/2024 [6].

The significant increase in interest and requested services during the pandemic reflects the active role of e-Governance in providing the necessary resources and information to citizens. The reduction of this number in 2024 can be interpreted as a consequence of a certain standard being reached in the provision of electronic services “Fig. 4”.

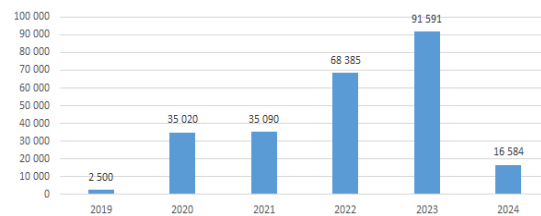


Fig. 4. Requested electronic services through the Unified Model. The data is current as of 02/20/2024 [6].

In the context of contemporary education and management of educational institutions, the electronic governance plays a significant role as a tool for supporting and optimizing various aspects of the educational process. Electronic governance was essential in coping with the crisis during the COVID-19 pandemic. By implementing distance learning in educational institutions, electronic governance allowed these institutions to continue functioning while there were restrictions on everyday activities. In Bulgaria, education was the first sector to mobilize after the announcement of the pandemic. Within 4 days of the announcement of the national quarantine, schools introduced distance learning, which covered large cities, rural areas and vulnerable groups. A non-governmental Roma organization [7] conducted a survey during the first days of the quarantine to assess the class attendance of students in 200 schools that educate children from vulnerable groups and schools that work with children whose parents have a relatively high level of education and social status. The results of the survey showed that the proportion of students participating in distance learning was promisingly high. Over 36% of schools surveyed were able to reach between 75% and 100% of their students through various forms of distance learning in the first 3 days. The percentage of schools that recorded low student participation in the first days was 6.6%. Two-thirds of schools combine internet-based techniques (giving assignments via Skype, Messenger,



etc. or e-classes on platforms such as Zoom) with printed assignments and paper lessons distributed by school mediators. The remaining one-third (32 percent) of schools use only Internet-based techniques. Among the identified obstacles to online learning is lack of appropriate devices - only in 22.34% of the schools more than 90% of the students have appropriate devices.

#### CONCLUSIONS

In conclusion, the present study highlights the significant role of the electronic governance in the context of crisis situations and emphasizes how appropriately integrated technologies can facilitate effective management in the face of disasters and threats. The analysis, based on a detailed examination of cases such as the COVID-19 pandemic and early warning systems in Chile, clearly illustrates how innovations in electronic governance help address the challenges associated with such emergencies. The review of successful practices and examples of crisis management aims to highlight the opportunities that technologies provide for optimizing the responses of society and institutions. Special attention has been paid to the example of Chile, from which valuable lessons can be drawn on building effective early warning systems based on sensors, software, and mobile communications. This observation supports our findings on the importance of electronic governance as a critical resource for maintaining public functionality and safety during crises. We have highlighted that electronic governance not only saves resources but also represents a key tool for overcoming challenges related to crisis situations. In conditions of economic instability or when rapid adaptation is required, electronic governance technologies offer some important solutions for process optimization and maintaining functionality of institutions. To move forward, it is essential to integrate new technologies such as artificial intelligence, blockchain, and robotics into electronic governance strategies. This will help in more flexible and rapid responses to emergencies. It is also crucial to invest both in electronic governance infrastructure and the improvement of staff training, which will ensure a smooth operation of systems during crises. Information security remains a priority, with effective data protection measures and counter-cyberattack strategies being essential for the continuous stability of electronic systems. Finally, strategies for improving access to electronic services for various social groups are critical for ensuring sustainable and effective management during crises. With collaborative efforts and an innovative approach, we can strengthen the resilience and efficiency of our societies in the face of future challenges.

#### ACKNOWLEDGMENTS

This publication is financed by the Ministry of Education and Science in implementation of the 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. The article reflects only the opinion of the authors. The Ministry of Education and Science is not responsible for its content.

#### REFERENCES

- [1] D. Pavlova, “Government in the Clouds. E-Government, Cloud Technologies and Successful E-Government Models”, Sofia, Academic Publisher “Za bukвите O Pismeneh”, 2021, ISBN: 978-619-185-456-1 (print), ISBN 978-619-185-457-8 (e-book) (in Bulgarian in original) Available: <https://drive.google.com/file/d/1ISxoUgOjbAlk5IpC8QbU7qYzRlk4wEV/view> [Accessed: Feb. 18, 2024].
- [2] Chile: Disaster Management Reference Handbook May 2017. [Online]. Available: [https://reliefweb.int/report/chile/chile-disaster-management-reference-handbook-may-2017?gad\\_source=1&gclid=CjwKCAiA8sauBhB3EiwAruTRJsCo5Pe936z6icXYp37ZTsZORlfnN17vLL0n31CzMV\\_rYx\\_sc-K5kRoCW0wQAvD\\_BwE](https://reliefweb.int/report/chile/chile-disaster-management-reference-handbook-may-2017?gad_source=1&gclid=CjwKCAiA8sauBhB3EiwAruTRJsCo5Pe936z6icXYp37ZTsZORlfnN17vLL0n31CzMV_rYx_sc-K5kRoCW0wQAvD_BwE). [Accessed Feb. 18, 2024].
- [3] A, Vodopyanov, Z, Dzhusupova and C. Flipov, “e-Government in Bulgaria: The Journey to 2020 and the Future Ahead (English)”. Washington, D.C.: World Bank Group. [Online]. Available: <https://documents1.worldbank.org/curated/en/650881631189254371/pdf/e-Government-in-Bulgaria-The-Journey-to-2020-and-the-Future-Ahead.pdf> [Accessed Feb. 18, 2024].
- [4] Department of Economic and Social Affairs, “United Nations e-Government Survey 2020”. Digital Government in the Decade of Action for Sustainable Development. United Nations. New York. 2020. [Online]. Available: [https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20\(Full%20Report\).pdf](https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf) [Accessed: Feb. 18, 2024].
- [5] Department of Economic and Social Affairs, “United Nations e-Government Survey 2022”. The Future of Digital Government. United Nations. New York. 2022. [Online]. Available: <https://desapublications.un.org/sites/default/files/publications/2022-09/Web%20version%20E-Government%202022.pdf> [Accessed: Feb. 18, 2024].
- [6] A Single, Model for Application, Payment and Receiving of Electronic Administrative Services. “Statistics of the provision of electronic administrative services through the Unified Model” [Online]. Available: <https://unifiedmodel.egov.bg/wps/portal/unified-model/unified-model/statistics/statistics/> [Accessed: March. 14, 2024].
- [7] D. Kolev and T. Krumova, “Distant learning: an opportunity for the development of education or a prerequisite for deepening educational inequalities”. 2020. [Online]. Available: <http://www.amalipe.com/index.php?nav=news&id=3690&lang=2> [Accessed: Feb. 18, 2024].
- [8] UN DESA, COVID-19 & Digital Government Compendium (2020), United Nations E-Government Survey 2020 - COVID-19 Questionnaire (Responses). 2020. [Online]. Available at [https://bit.ly/EGOV\\_COVID19\\_APPS](https://bit.ly/EGOV_COVID19_APPS) [Accessed: Feb. 18, 2024].

# Complex of Activities Supporting the Management of the Radio Frequency Spectrum in Military Operations

**Nikolay Petrov**

Department of Communication and Information Systems  
"Vasil Levski" National Military University  
Veliko Tarnovo, Bulgaria  
nmpetrov@nvu.bg

**Abstract.** *The dependence of military capabilities on the radio frequency spectrum, as well as the saturation of the spectrum with different users, are part of the realities and challenges of the modern battlefield. This requires the Alliance and the coalition forces to have an effective radio frequency spectrum management concept, and the application of uniform rules will ensure the achievement of electromagnetic compatibility, which is the ability of all units of radio electronic equipment to function when working together in an electronic environment.*

**Keywords:** *radio frequency spectrum, frequency management, spectrum management cycle, military radio communications.*

## I. INTRODUCTION

Radio communication is one of the main types of communication and a means of commanding formations in modern operations. The term "radio frequency spectrum" (RFS) generally refers to the frequency range from 3kHz to 3000GHz that can be used for wireless communication and information transmission. RFS is a natural and limited resource, allowing it to be used simultaneously by multiple users, which can lead to the appearance of mutual interference. In order to prevent the occurrence of this type of interference, it is necessary to ensure conditions for coordinated and harmonized use of the RFS, which is achieved through the management of the RFS. RFS management encompasses any of the spectrum planning, coordination and regulation decisions or actions that directly determine how it will be used.

## II. MATERIALS AND METHODS

For the development of the proposed in the report set of activities supporting the management of the radio frequency spectrum in operations, a review of the information in the scientific literature examining the

nature and classification of RFS, as well as the problems related to the saturation of the spectrum, was made. A study and analysis of the publications and documents regulating spectrum management in the interest of national security and defence, and in particular in the conduct of operations, have also been carried out.

The dependence of military capabilities on the RFS, as well as the saturation of the spectrum by different users, is one of the realities and challenges of the modern battlefield.

This requires the management of the RFS to ensure the most effective and efficient use of spectrum and meeting the frequency resource needs of military users, while ensuring the necessary coordination with the host countries in the area of responsibility.

As a result of RFS management, mutual interference between friendly transmitters, loss of communication capability due to spectrum oversaturation, and interference with or jamming of enemy transmitters that are sources of intelligence information are avoided.

According to [4], RFS management is understood as "the process of identification and effective use of available RFS for military purposes". This process is related to policies and rules on the allotment of frequency bands, the allotment of radio frequencies or radio frequency channels, and the appropriation (assignment) of frequencies.

RFS management is part of communication and information support, therefore the exchange of information in the interest of the command-and-control system (C2) will depend on the timely and reliable assignment of frequencies and the correct distribution of radio communication assets in the area of operation.

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8232>

© 2024 Nikolay Petrov. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

The process of managing RFS in the Alliance for each operation can be presented as a cycle that contains four phases:

- Preliminary planning phase - related to the collection of data necessary for the management of RFS during the operation.
- Planning phase – the main objective is to prepare a management plan for RFS. During this phase, frequencies and channels are allotted and tables for frequency allotment and assignment are drawn up, in accordance with spectrum management policies and procedures. The result of the activities carried out in this phase is the "RFS Management Plan", which depends on the type of operation and is prepared by the RFS Management Unit as part of the planning process.
- Implementation phase of the operation- Upon reaching the operation area, the implementation of the plan drawn up in the previous phase shall be carried out. During this phase, the RFS Management Unit takes action to: establish and maintain close contact with the authorities responsible for the radio spectrum of the receiving nation and neighbouring nations, resolve conflicts in the use of RFS between users, update the HRS management plan.
- Transition phase - the frequency resource used during the operation is "transmitted" for reassignment in order to be accessible for other purposes and users.

### III. RESULTS AND DISCUSSION

Based on the information obtained from the study of the documents regulating the use and management of RFS in the armed forces, this report proposes a set of activities to achieve effective management of RFS in operations, which aims to:

- establish the necessary organization of the radio communication of the formation - determination of the number of networks, the correspondents who will use them, the distance of communication and the type of information exchanged in them;
- analyse the conditions for the use of RFS in the area of operation;
- plan the necessary radio communications;
- plan the allotment of the radio frequency spectrum;
- assign radio frequencies to correspondents.

The proposed complex consists of ten activities listed below:

**Activity 1.** Definition of the specifics of the operation and planning guidelines.

The activity covers familiarization with the received incoming documents on the planning of the operation - the Plan for the operation and Annex Q [1] from the senior authority, familiarization with the frequency distribution tables in the area of the operation, the requirements of the formation's C2 and the available radio equipment.

From the input documents it should be clearly understood the operational area to which the operation belongs, the type of operation – joint or allied, the

presence of support from the host nation, the functions, and responsibilities of the different countries to manage the spectrum within the deployed multinational forces.

According to modern doctrines, military operations should be conducted with the use of joint or allied forces. This requires the planning, coordination, and management of the RFS in coalition military operations to be delegated to a leading nation, with the active and constant participation of all coalition members. In this case, the leading nation is responsible for relations with the civilian administration and provides the framework for the management of the RFS for the deployed military forces.

A leading nation can demand radio frequency resources for exercises or most military operations other than war. Operations that preclude prior coordination with a host nation, such as forced entry, will require the frequency manager to evaluate the electromagnetic environment and spectrum use in subsequent activities.

**Activity 2.** Collection of information on the RFS.

Information shall be collected regarding the frequencies used for radio exchange in the area of operation, as well as the frequencies for the operation of the own radar, navigation, and weapon systems. This activity continues until the start of the operation and assists in planning.

The product generated by the information gathering activity is a database in the SPECTRUM XXI application, which contains data on RFS and its use by all own military and civilian, available adversary and neutral forces in the operation area.

**Activity 3.** Summary and analysis of information on RFS.

The activity determines the resource from the RFS required to maintain the C2, the need to prepare frequency sharing plans and reuse them in the area of operation.

This process requires compilation and analysis of the generated data through Activity 2 and helps develop the tables for the allotted frequencies for the subordinate formations and the assigned frequencies for work for the radio resources.

**Activity 4.** Determination of the factors influencing the organization of radio communication.

The factors influencing the organization of adaptive radio communication in the area of operation can be divided into four areas: Political and Legal Factors, Social and Environmental Factors, Economic Factors and Technical Factors.

Their identification helps to correctly establish the propagation of radio waves, electromagnetic compatibility, operating frequencies, the type of antennas, the range of communication and vulnerability to interception and suppression by enemy electronic warfare forces.

**Activity 5.** Development of the scheme of radio communications for the operation.

The activity concerns the development of the scheme of radio communications according to the principles for organizing radio communication, the frequency resource that has been allotted and the requirements of the C2.

**Activity 6.** Assignment of frequencies.

An important point related to the management of RFS during the activity is the development of frequency assignment tables for each of the courses of action (CA).

The table of allotted frequencies and ordered radio networks and directions is the most critical resource available to the CIS planner in the CIS department, because it is the basis for nominating appointments without interference, providing analyses of the impact of electromagnetic warfare operations, as well as identifying and solving interference problems.

During the activity, the table of assigned frequencies of radio stations is prepared. Most often, frequencies are determined by the table of allotted frequencies brought down by the senior authority in Annex Q.

**Activity 7.** Development of a management plan for the RFS.

A plan is being drawn up for the use of available resources from the RFS, which will be used to organize radio, radio relay and satellite communication in the operation. The basis for the plan is the incoming documents from the senior authority and the results obtained as a consequence of the previous activities.

The RFS management plan shall include the tables of allotment and assigned frequencies of the means of communication, describe all spectrum management actions, and indicate the procedures for reporting interference and the proposed steps for their resolution.

The assignment of frequencies for the operation of radio equipment in radio networks and directions is the actual implementation of the RFS management plan for the operation.

**Activity 8.** Development of communication instructions for work.

The activity should cover the related to the planned adaptive radio directions and networks: callsigns, network identification rules, the direction output order, the rules for changing the operating frequencies, the coding rules and the entry and change of the cryptographic keys for the operation of the crypto modules.

**Activity 9.** Preparation of a list of prohibited frequencies.

The list is a product that protects radio communications networks from interference and suppression by one's own electronic warfare forces during exercises or operations.

**Activity 10.** Interference analysis, interference conflict resolution and their reporting.

Various factors such as impact from the adversary, unauthorized users, incorrectly assigned frequencies, or equipment problems can create interference. The person responsible for RFS shall analyse and define the electromagnetic working environment in order to determine the cause of the interference. Solving them is a

daily activity once the forces are deployed and operating in the area of operation. One of the actions that can be taken when interference occurs is the change of the working frequencies of the correspondents, which is reflected in the table of assigned frequencies.

After performing an interference analysis, a report is always created to document the results. These reports are stored in a database that can be used as a history of interference problems. The purpose of the interference reports database is to provide the person responsible for the RFS with information on previous incidents and the steps taken to resolve them.

In conclusion, it can be said that some of the activities in the complex thus proposed, related to the management of RFS in operations, can be carried out simultaneously, while others occur only sequentially, after receiving an outgoing result from the previous ones.

## CONCLUSION

Effective RFS management is important for the success of the entire spectrum of operations and exercises conducted by the armed forces.

The proposed set of activities aims to establish the necessary organisation of radio communications in the conduct of operations, to assign radio frequencies to correspondents and to ensure the achievement of electromagnetic compatibility (EMC), representing the ability of different units of radio-electronic equipment to work well when operating together in an electronic environment.

## ACKNOWLEDGMENTS

The publication and dissemination of the research results was carried out thanks to the support of the National Science Program "Security and Defense", approved by Decision №171/21.10.2021 of the Council of Ministers of the Republic of Bulgaria.

## REFERENCES

- [1] N. PAVLOVSKI, *Operations Planning at Tactical Level by Land Forces Units*. Veliko Tarnovo, Vasil Levski National Military University Publishing Complex, 2023, p.282 (ISBN 978-954-753-365-3 – soft cover and ISBN 978-954-753-366-0 – CD) [ПАВЛОВСКИ, Н. *Планиране на операциите на тактическо ниво от формированията на Сухопътни войски*. Велико Търново, издателски комплекс НВУ Васил Левски, 2023, с. 282. (ISBN 978-954-753-365-3 – мека корица и ISBN 978-954-753-366-0 – CD)]
- [2] APP-28, *Tactical planning for land forces*, Edition A Version 1, NOVEMBER 2019.
- [3] ATP 6-02.70 *Techniques for Spectrum Management Operations*. October 2019.
- [4] ITU Radio Regulations (4 Vol. Set), 2016 Edition.
- [5] *Spectrum management in military operations*, NSO, 2017.

# A Screening Method for C2 Expert Assessment

Ivo Radulov

Rakovski National Defence College  
Defense Advanced Research Institute  
Sofia, Bulgaria  
[i.radulov@rndc.bg](mailto:i.radulov@rndc.bg)

Teodora Georgieva

Rakovski National Defence College  
Defense Advanced Research Institute  
Sofia, Bulgaria  
[t.georgieva@rndc.bg](mailto:t.georgieva@rndc.bg)

**Abstract.** Although it is widely recognized that simulations based on particular scenarios are the best Measures of Force Effectiveness (MoFE) and Measures of Command and Control Systems (C2) Effectiveness (MoCE), a generalized assessment of the entire C2 system or certain its parameters for particular practical and research purposes is required. Current report presents a screening method for C2 expert assessment, built on the basis of a detailed analysis of the Doctrine of the Bulgarian armed forces in its chapter "Leadership, command and control of the armed forces". The Measures of Performance (MoP), namely the focus on internal system structure, characteristics and behaviour and the Dimensional Parameters (DP) - the focus on the properties or characteristics inherent in the physical C2 systems are used as underlying, intrinsic principles. The purpose of constructing and applying the method is to present a general rough picture of the state of C2 and to mark the areas of its strengths and weaknesses. Through changes in the instruction and in certain items, the questionnaire can be applied to different contexts. The separate structural blocks of the questionnaire assess aspects of the three levels of commands and the complex capabilities of their bodies, the practical and technical parameters of the available Communication and Information system (CIS), etc. After a validation process, the method can be used as a convenient tool for educational, scientific and practical purposes.

**Keywords:** expert evaluation, C2, CIS, screening method.

## I. INTRODUCTION

Command and control system (C2) represent complex systems of amplification of the basic human decision-making processes through procedures, organizations, equipment, threat assessment, and resource allocation to manage human factor and logistics in a real-world environment and actual time to achieve a defined strategic, operational, or tactical objective [1]. Their architectural complexity and focus on the achievement of multidirectional goals and tasks in the context of scenarios with different intensity and multifactorial contextual expressiveness excludes the existence of a single conceptual framework for the construction of a methodology that evaluates the overall effectiveness and performance of C2 in particular situations [2]. Regardless

of the fact that the method of modelling and testing scenarios is perceived as an invariable means of predicting the sequence of events in a real theater of combat operations, for educational and practical purposes there is a need to construct simplified tools for carrying out certain analyses.

## II. MATERIALS AND METHODS

In current report, simplification in developing measurement instrument (questionnaire) was achieved through the application of three criteria: doctrinal, screening and expert. The Doctrine of the Bulgarian Armed Forces (BAF) is "an officially approved national publication describing how the acquired capabilities can be used in contemporary circumstances, taking into account the particular organization and technologies introduced. Therefore, its primary purpose is to assist commanders in the performance of their major functions of command and control of troops". Chapter 9 of the document presents precisely the structure, principles and other main characteristics of the BAF's C2 [3, p. 6].

The second characteristic of the developed questionnaire is its screening nature. In general, screening instruments are short and easy to administer, used as the first step in the assessment process [4]. Their purpose is to determine the degree or likelihood that a particular object or subject of assessment possesses a particular characteristic, potential needs, strengths or limitations. Objects selected at this first step undergo further formal in-depth evaluation. Professionally constructed screening questionnaires have high sensitivity to the intended measurement questions and poor specificity in adopting a broader perspective of measurement.

The third feature of the newly created tool is the application of the potentialities of expert assessment [5]. The experience and knowledge of well-chosen experts who are able to quickly and accurately identify certain problems is important for deriving their prioritization and conclusions for overcoming.

The purpose of the tool presented below is to provide a rough assessment of the degree of functionality of the

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8210>

© 2024 Ivo Radulov, Teodora Georgieva. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

Bulgarian C2: the extent to which the principles of C2 functioning defined in the Doctrine of the BAF are actually available and implemented in the form of resources, infrastructure, information connectivity, interaction between the three levels of the chain of command and so on [7]. The objectives of the study is to identify areas of deficits and strengths, as well as to obtain a screening assessment of the system's readiness to perform functions in a wartime environment, military situation or military crisis.

Two types of measures are applied in the description of the system: Measures of Performance (MoP) that focus on internal system structure, characteristics, and behavior and Dimensional Parameters (DP) that focus on the properties or characteristics inherent in the C2 system [6]. Pursuant to NATO COBP the structural representation of DP and MoP among other MoMs can be seen in fig. 1.

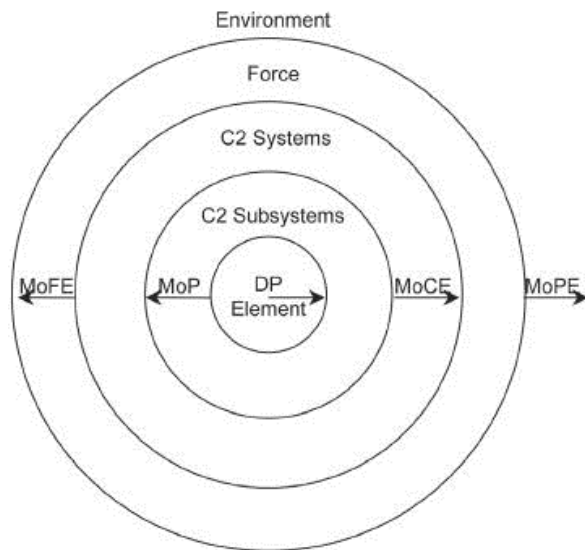


Fig. 1. Relationships of Measures of Merit (MoM)

According to the authors all the structural components of the system included for measurement in the questionnaire (the three levels of command, infrastructure, CIS) could be considered as characteristics of DP, while the items on capabilities to make connections between the individual components of the C2 could rather be perceived as related to the level of performance of the system at the task level (without a specified final desired state), therefore appear to be more relevant to the MoP.

Generally, MoMs are used to compare different options on equal terms and serve a wide range of purposes. Regarding the presented questionnaire, the following objectives are relevant:

- Establishing a standard or expectation of performance (for new requirements);
- Establishing the performance limits of the system, as well as the effects of the imposed restrictions;
- Evaluation of the use of a system in new or unexpected areas of application;
- Identifying potential weaknesses in specific areas of a system;

- Evaluation of the effectiveness of human decision-making in the C2 cycle.

The Expert Assessment Card is intended for completion by experts holding positions in the Directorates of the Ministry of Defense and commanders of military formations. In the current report, the items are oriented to the experts' assessments of the possibilities of transforming the C2 from a peacetime to a wartime variant. Five points Likert scale response options are used: *weak, rather weak, medium, rather high, high* for all questions. The original form of presentation of the questionnaire for assessment by the experts is in tabular form.

Eight blocks of questions that concern different aspects of C2 functioning will be presented.

The complete theoretical model on which the questionnaire is built is presented in Table 1.

TABLE 1. MODEL OF QUESTIONNAIRE

Data Types	Table Column Head
	Assessment of the:
Q/N	C2 contribution to the <i>strategic level</i> of command of the BAF
Q/I	Complex capabilities/the most pronounced deficits of C2 to support <i>strategic</i> level authorities
Q/N	C2 contribution to the <i>operational</i> and <i>tactical</i> level of command of the BAF
Q/I	Complex capabilities / the most pronounced deficits of C2 to support <i>operational</i> level authorities
Q/N	Complex capabilities of C2 to support <i>operational</i> level bodies of the BAF: JFC, LF, AF, N, JSOC, LSC, CISDC, SDSMD
Q/I	Complex capabilities / the most pronounced deficits of C2 to support <i>tactical</i> level authorities
Q/N	Complex capabilities of C2 to support <i>tactical</i> level bodies of the BAF: JFC, LF, AF, N, JSOC, LSC, CISDC, SDSMD
Q/N	General capabilities of C2 to support the <i>strategic level</i> of command of the BAF
Q/N	C2 infrastructure
Q/N	Elements and principles of C2 functioning
Q/N	Available CIS in the BAF as a core element of C2
Q/N	CIS capabilities available to the BAF compared to the ideal one
Q/N	Technical parameters of the CIS available to the BAF compared to the ideal one

Abbreviations: Q/N (quantitative questions); Q/I (qualitative questions); Bulgarian Armed Forces (BAF); Joint Forces Command (JFC); Land Forces (LF); Air Force (AF); Navy (N); Joint Special Operations Command (JSOC); Logistics Support Command (LSC); Communications and Information Support and Cyber Defence Command (CISDC); The structures directly subordinated to the Minister of Defence (SDSMD).

### III. RESULTS AND DISCUSSION

The quantitative and qualitative blocks of questions are presented below.

#### 1. Assessment of the C2 contribution to the strategic level of command of the BAF

Instruction: How do you assess the capabilities of BAF C2 to support strategic command in the wartime activities/areas described below?

1A). Q/N. (10 items): Increasing of the BAF's combat and operational readiness/ Implementation, supplement, adaption or creation of new strategic plans/ Creation of command and control models adequate to the situation and the pursued goals in: a scenario with a dominant participation of the LF component/ a scenario with a dominant participation of the AF component/ a scenario with a dominant participation of the N component/ a scenario of joint operations/ Adoption of adequate and expedient decisions that operate within the adversary's decision cycle/ Accurate assessment of the parameters of the BAF' participation in operations (operational command, authority, command structure)/ Effective coordination with the commands at the operational level (the commander of the JFC, the commanders of the military services) and his directly subordinate formation/ Effective management of information, psychological and special operations/ Accurate assessment of the moment to activate forces and their composition in operations/ Identification of the proper application of the rules of engagement of military forces / Development of effective strategies to adapt to the challenges of urban warfare.

1B). Q/l. *How do you assess the complex capabilities of C2 to support strategic-level authorities in a wartime situation? In which area are the most pronounced deficits observed?*

## **2. Assessment of the C2 contribution to the operational and tactical level of command of the BAF**

*Instruction: How do you assess the capabilities of BAF C2 to support operational and tactical command in the wartime activities/areas described below?*

2A). Q/N. (13 items): Implementation of strategic command's plans by operational command/ Planning and operations' conduct by the JFC and the military services' commands at the operational level/ Provision of effective coordination and interaction of the JFC with the military services' commands and assigned formations/ Support for the integration of the operation unit with the JFC and the military services' headquarters/ Coordination and interaction at the operational level of the military services' commands components and the SF component/ Coordination and interaction of the military services' commands components with the main combatant headquarters staff and the deployment staff/ Provision of information and expertise from the AF command to the military services' commands components/ Conduct of independent or joint N command operations through the Maritime Operations Center/ Conduct of special reconnaissance and surveillance by the SF component command/ Undertake direct action and military support by the SF component command/ Conduct of the SF command coordination with the JFC and the military services at the operational level/ Accomplishment of command and control by the SF command in the case of conducting independent or joint operations with specialized coalition/alliance military forces/ Coordination between the operational command and the tactical command/ Accomplishment of the tactical command and control by the commanders of military formations with their subordinate military formations.

2B). Q/l. *How do you assess the complex capabilities of C2 to support operational level authorities in a wartime situation? In which area are the most pronounced deficits observed?*

2C). Q/l. *Please rate the complex capabilities of C2 to support the operational level authorities of the BAF in a wartime situation of: the JFC, the LF, the AF, the N, the JSOC, the LSC, the CISCDC, and the SDSMD.*

2D). Q/l. *How do you assess the complex capabilities of C2 to support tactical-level authorities in a wartime situation? In which area are the most pronounced deficits observed?*

2E). Q/l. *Please, assess the complex capabilities of C2 bodies to support the tactical level of the BAF in a wartime situation of: the JFC, the LF, the AF, the N, the JSOC, the LSC, the CISCDC, and the SDSMD.*

## **3. General assessment of the capabilities of C2 to support the command of the BAF**

*Instruction: What is your assessment of the BAF C2's capabilities to support command and control in the wartime activities/areas described below?*

Q/N. (15 items): Joint fire support/ Vertical and horizontal coordination of fire support/ Adoption of measures appropriate to the risks and threats to ensure the security of troops and forces/ Provision of reliable, accurate and timely Intelligence information/ Provision of reliable, accurate and timely information by the Counterintelligence / Coordination of the JFC and the military services commands with the intelligence's command and control/ Coordination of the JFC and the military services commands with the counterintelligence's command and control/ Coordination with allied, coalition and multinational operations/ Functional analysis of the operational requirements necessary to perform a given task and determining the necessary CIS for support/ Logistics assurance to ensure efficient use of resources/ Management of the missile defence for the airspace defence/ Management of the rear services protection/ Management of the critical infrastructure protection/ Ensure of the coordination with other governmental bodies and the private sector/ Ensure of the adequate electronic protection of troops.

## **4. Assessment of the C2 infrastructure**

*Instruction: What is your vision for the BAF's capabilities to build the infrastructure for wartime C2 operations?*

Q/N. (13 items): Deployment of stationary control posts for the LF command component during independent military operations/ Deployment of field control posts of the LF command component during independent military operations/ Deployment of protected control posts for the Navy operations/ Support for the functionality of the Maritime Operations Center for the implementation of independent or joint Navy operations/ Maintainment of the operation of the Maritime Operations Center as an outsourced control posts for the JFC/ Maintainment of the fire support and liaison centers/ Deployment and maintainment of the stationary and mobile CIS outposts

with deployment capabilities/ Deployment and maintainment of a CIS that is integrated with weapons control systems and sensor systems/ Deployment and maintainment of a network-centric information environment, providing integration of the used information networks, access to a common operational picture and sharing of the extracted information/ Deployment and maintainment of the logistics support units/ Deployment and maintainment of the strategic CIS/ Deployment and maintainment of an operational CIS/ Deployment and maintainment of a tactical CIS.

##### **5. Assessment of the elements and principles of C2 functioning**

*Instruction: Please provide your comprehensive assessment of the overall performance of BAF's C2 and its base structural components in a wartime situation.*

Q/N. (19 items): The extent to which the number of the personnel involved in C2 ensures its effective functioning/ The degree to which the preparedness of the personnel involved in C2 ensures its effective functioning/ The capabilities of C2 equipment ensures its effective functioning/ The capabilities of C2 equipment ensures its effective functioning/ The degree to which the clarity, detail and comprehensiveness of the procedures governing C2 ensures its effective functioning/ The degree of resilience of C2 (the capabilities and resources to timely increase the number of control points that the adversary will seek to neutralize/reduce)/ The degree of resilience of the C2 communication networks/ The degree of stability of the interrelationships between the C2 headquarters/ The capabilities of the BAF' command staff to maintain the principle of continuity in leading the subordinate troops and forces/ The preparedness of the BAF' command staff to implement the principle of operability in a wartime situation (timely response to changes in the situation and successful implementation of the assigned tasks)/ The capabilities of C2 to keep it secret, including the concept (plan) of the operation, the main arrangements for the preparation and conduct of the operations/ The designed interrelationships between C2 structural components are simplified and logical/ The flexibility and speed of C2 in its transition from peacetime operation to wartime operation/ The flexibility of C2 in the "supported" - "supporting" relation and the possibility of reconfiguring part of the system in the course of operations/ The degree to which the clear chain of command of C2 regulated in the normative documents is able to guarantee the efficiency of the system's functioning/ The capabilities of C2' all elements (personnel, infrastructure, equipment, technical support, procedures) to continue functioning in an adverse environment, under threat, and to recover after inflicted losses (principle - continuity of C2)/ The extent to which the reserve is able to ensure C2 continuity/ The extent to which substitution rights in the chain of command are clearly defined for all levels of command/ The degree to which the complex capabilities of the command structure is able to integrate various military components or structures while at the same time being itself integrated into other structures/ The possibilities of procedures (orders) to regulate decentralized task execution.

##### **6. Assessment of the available CIS in the BAF as a core element of C2**

*Instruction: Please provide your comprehensive assessment of the overall performance of the BAF's CIS and its basic wartime structural components.*

Q/N. (12 items): Overall CIS effectiveness (timeliness, stealth, combat readiness, resilience and mobility)/ Timeliness of CIS - the possible state of the system due to the impact of the enemy's means of striking/ Resilience of the CIS - the ability of the system to perform the assigned tasks in conditions of impact of all the confounding factors of the enemy/ Modern capabilities of the CIS to enter data for: terrain with locality data; the types of armament, the organizational units, the order of battle, the scenario of combat operations/ Degree of information connectivity of the command system/ Structural reliability of the system of control posts/ Opportunity of all the elements of Bulgarian army divisions to share and exchange information about the operational situation/ Possession of the complete package of capabilities for integration and management of the combat potential of all the elements of the battle space/ Availability of a relation between support capabilities and operational activities/ Reliability of control posts/ Information connectivity of control posts (degree of information accessibility of a control posts to each information direction).

##### **7. Assessment of CIS capabilities available to the BAF compared to the ideal one**

*Instruction: How do you assess the CIS capabilities available to the BAF compared to the ideal?*

Q/N (22 items): Tactical picture management/ Support planning and decision making/ Operational management (management of combat or non-combat operations)/ Peacetime, wartime and crisis resource planning and management/ Creation, formatting, authentication and sending of orders, reports and messages/ Dissemination of information and data in real time/ Maintain information layers including planning and control of tactical maneuver, intelligence, order of battle, paint sustainment, chemical defense, and air defense and air defense operations/ Personnel management/ Analysis of the area, conditions for the movement of forces, transport/ Storing the information and having resources to use it to support planning and decision-making processes/ Force organization management/ Sustaining non-military operations/ Fire support planning and management/ Air defense planning and management/ Holds functions providing peacekeeping operations, including civil-military interaction/ Holds perfectly working communication/ The staff is fully competent to work with the system/ Requests to higher levels do not require waiting, but are processed promptly/ The necessary decision support systems are available/ Holds functions providing continuous information about air, land and water/ None of the wars C2 is leading is not effective against its own forces/ The available CIS is integrated, provides opportunities to build an object model, a dynamic model and a functional model [9, 10].

##### **8. Assessment of technical parameters of the CIS available to the BAF compared to the ideal one**



*Instruction: How do you assess the technical parameters of the CIS available to the BAF compared to the ideal?*

Q/N (9 items) Data transfer rate/ Transmission time/ Sensor coverage/ Detection capabilities/ Mean time between failures/ Average recovery time/ Speed (planning time, order time, response time)/ Accessibility (availability)/ Situational clarity (timeliness of situational update, timeliness of distribution of orders) [9, 10].

#### CONCLUSION

The rapidly changing geostrategic environment and the rhetoric of our official authorities to make progressive contribution to NATO's collective defence require an accelerated development of national defence capabilities [10]. In the considered context of objective circumstances, the proposed tool can be used as a screening method for a quick assessment of strengths and deficiencies in the C2. Decision making is at the heart of the command and control process. CIS as a core element of C2 must be designed primarily to provide effective and responsive decision support. To achieve this goal, the system must include support for personnel whose mission is to provide the various inputs needed to make command and control decisions, some driven by the personnel's functional responsibilities and others by specific inquiries posed by the commander [11]. All these characteristic are included as options for assessment in the questionnaire.

So far, the methodology has been approved by a small number of experts. A future step in its development is validation in a larger sample of experts occupying command positions. Subsequent addition and modification of the content of the items will follow. After completing the validation process, the methodology can be used as a tool for educational, scientific and military expert 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] C. J. Harris and I. White "Expert systems in C2 systems", *Advances in Command, Control and Communication System*, January 1987. P. Peregrinus, on behalf of the Institution of Electrical Engineers, London, U.K.
- [2] B. Claverie and G. Desclaux, "C2 - Command and Control: A System of Systems to Control Complexity", *American Journal of Management* vol. 22(2), pp. 45-63, 2022.
- [3] National publication of the Armed Forces of the Republic of Bulgaria. NP – 01. "Doctrine of the Armed Forces of the Republic of Bulgaria". Issue (A), November, 2017. [https://ccdcoc.org/uploads/2018/10/Bulgaria\\_Bulgarian-Armed-forces-doctrine\\_2017\\_original.pdf](https://ccdcoc.org/uploads/2018/10/Bulgaria_Bulgarian-Armed-forces-doctrine_2017_original.pdf).
- [4] A. E. Boone, W. L. Henderson, and W. Dunn, "The Issue Is— Screening tools: They're so quick! What's the issue?" *American Journal of Occupational Therapy*, vol. 76, pp. 1-5, 2022. <https://doi.org/10.5014/ajot.2022.049331>.
- [5] N. J. Lambert and U. Candan, "Analysis & Evaluation of the Immediate Reaction Task Force (Land) Command and Control Concept: Applying the COBP". Paper presented at the RTO SAS Symposium on "Analysis of the Military Effectiveness of Future C2 Concepts and Systems", held at NC3A, The Hague, The Netherlands, 23-25 April 2002, and published in RTO-MP-117.
- [6] D. Alberts, T. Bailey, P. Choinard, A. Tolk, G. Wheatley and J. Wilder, "NATO Code of Best Practice for C2 Assessment". *Computational Modeling and Simulation Engineering Books*, 2002. [https://digitalcommons.odu.edu/msve\\_books/13](https://digitalcommons.odu.edu/msve_books/13).
- [7] H. Chen, T. Li, L. Zhu , T. Jiang, "Function Analysis of Command and Control System in Intelligent War", *Journal of Physics: Conference Series* 1684 (2020) 012147 IOP Publishing doi:10.1088/1742-6596/1684/1/012147.
- [8] K. Kalchev, "Influence of the communication information system on the combat capabilities of military formations". *Proceedings of the International Scientific Conference Forum "Defense Technologies 2020"*, pp. 260-263, Shumen 2020, ISSN 2367-7902.
- [9] I. Hristozov, "Architecture of the management system of the Bulgarian Army in the Mur offensive operation". *Collection of reports from the annual university scientific conference May 27-28, 2021, item 6, Scientific direction "Security and Defense*, pp. 142-154, National Military University, Veliko Tarnovo, ISSN 1314-1937.
- [10] Z. Zdravkov, A. Atipova and S. Stoykov, "Analysis of plans for modernization, construction and development of the defense and armed forces of the Republic of Bulgaria 2003-2019", *Compendium of reports from the Annual student scientific session of the "Command and Staff" Faculty, on the topic "Modern aspects of security - challenges, approaches, solutions"*, pp. 367-374, 2022.
- [11] L. D. Diedrichsen, "Command and control operational requirements and system implementation", *Information and security. An International Journal*, vol. 5, pp. 23-40, 2000.

# Modelling of Capability-Based Defence Planning Processes

Ivo G. Radulov

Rakovski National Defence College  
Defence Advanced Research Institute  
Sofia, Bulgaria  
[i.radulov@rmdc.bg](mailto:i.radulov@rmdc.bg)

**Abstract.** The realization of the planned level of effectiveness of decisions in the field of defence, and thus the development of the necessary defence capabilities, depends and is determined to a significant extent by the quality of defence planning and the implementation of the transformation of the armed forces. This feature is of crucial relevance in the uncertain future security environment. The preservation and development of defence capabilities in response to threats and commitments to national and global security, under conditions of severe constraints on available resources, necessitates a search for adequate methods to enhance the effectiveness of the defence planning process.

The purpose of this publication is to present an revised model of the Defence Planning System used in the Ministry of Defence and the Bulgarian Army. The model is presented with tools for formal description and analysis. An analysis of the activities is performed. The formed model of the future state (To-Be) has been verified for adequacy, completeness, and consistency using the presented methodology.

Revised model has been adopted as the main methodology for the Strategic Defence Review of the Ministry of Defence and the Bulgarian Army from 2019-2021.

**Keywords:** Modelling, Capability-based defence planning, E-nets.

## I. INTRODUCTION

NATO countries have well-established defence planning processes, procedures and methods. Using these tools, participants in this process determine the capabilities required of their armed forces so that they can meet the standards set over the long term. It has been proven in practice that when it comes to the actual acquisition and development of defence capabilities, the necessary resources are always insufficient. The result is a capability gap. These gaps take various forms and dimensions, most often in the form of shortages of

weapons and equipment, combat training, logistic support and communications, incompatible and/or vulnerable communication and information technologies, command and control systems, etc. Other negative examples of shortfalls resulting from budget spending on the purchase of assets and services that do not contribute to the development of the capabilities actually required by the armed forces (AF) are no exception. The result of all this is incapable formations and structures that are unable to perform their missions and tasks.

The purpose of the study is to propose an adequate defence planning system model. To achieve this goal, a methodology for the analysis and formal description of the model will be used.

## II. MATERIALS AND METHODS

The following formal description and analysis methods were used to find realistic solutions:

**IDEF0.** IDEF0 is a set of elements of a system or a domain. It was developed based on the ICOM (Input, Control, Output, Mechanism) concept and is integrated in the architectural approach to represent activities in an organization [8].

IDEF0 is used to describe the activities in the system as well as the end products.

IDEF0 is a modelling tool based on a combination of graphics and text. IDEF0 are presented in an organized and systemized manner to support analysis, provide logic for potential changes, define requirements, or support the design of individual system levels and integration activities.

An IDEF0 model is composed of a hierarchical series of diagrams that progressively reveal increasing levels of detail describing functions and their interfaces in the context of the system.

**Graphschemes of the algorithm.** They are used to describe sequential and parallel algorithms [9]. Their main elements describe: 1) the places of logical branching of the algorithm; 2) the places of joining

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8214>

© 2024 Ivo G. Radulov. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

parallel sections of the algorithm; 3) the execution of certain actions (steps) of the algorithm.

Using graphschemes to describe algorithms (especially in programming systems) provides the following advantages:

- better tractability;
- simplicity in program implementation;
- verification of the correspondence between the algorithm and its implementation;
- fast and natural transition to description using

Logical schemas of the algorithm (LSA) and Matrix schemas of the algorithm (MSA) to prove completeness and consistency of the model.

**Tabular graph of the algorithm.** Serves for description of interactions. It consists of two types of elements.

- static: 1) a single timeline - to account for the beginning and end of the execution of the interactions; 2) a table in which each column corresponds exactly to one user or resource.

- dynamic: 1) vertical arrows - placed in columns of the table corresponding to the interaction that is being executed, with the projections of the two ends of the arrow on the single timeline indicating the start and end of the interaction; 2) horizontal arrows (starting in one column and ending in another column) - reflect the relationships between interactions and their input and output parameters.

**Matrix schemes of algorithms.** Matrix schemes of algorithms have universal application. They can be used to describe and analyse processes, program systems, are used for structural representation of algorithm interaction (operations, logical conditions and transitions), facilitate program implementation and serve to prove the completeness and consistency of the model.

The matrix scheme of the algorithm (MSA) is given by a square matrix, on each row of which an operator in the order  $A_0, A_1, \dots, A_{k-1}$  is matched, and on each column -  $A_1, A_2, \dots, A_k$ . In element  $a(i, j)$  of the matrix a logical condition (function) is written.

A properly constructed MSA possesses characteristic features that allow to check such important properties of the algorithm as completeness and consistency conditions [10]. The completeness condition is satisfied exactly when the disjunction of all elements of a row is equal to 1. The non-consistency condition is satisfied exactly when the conjunction of any two elements of a row is equal to 0.

**Evaluation Nets.** Defined by Nutt and Noe, E-nets are a modelling tool that further develops Petri nets in terms of the types of transitions and conditions in them [3, 4, 5, 6]. They belong to the simulation modelling tools and allow to represent not only the dynamics of processes (synchronous and asynchronous) but also the way to control them and the associated data transformation procedures. It is appropriate to use them in the analysis of

models with the presence of asynchrony, parallelism, non-determinism of processes and dynamics of functioning. Describe them with simple syntax and clarity.

E-nets provide theoretical insight into the structure and dynamics of systems of discrete events expressed by graphs. They can be used to provide a mathematical description of the processes to be analysed and to provide an assessment of functionality.

E-nets are defined as ordered sevens:

$Ne = \langle B, B_p, B_r, D, F, H, M_o \rangle$ , where:

$B$  is a non-empty finite set of symbols called positions;

$B_p$  is a set of peripheral positions, a subset of  $B$ ;

$B_r$  - set of decision (control) positions, a subset of  $B$ ;

$D$  - a non-empty finite set of transition descriptions  $di: di = (s, t(di), p)$ , where  $s$  is a transition type,  $t(di)$  is a transition time, and  $p$  is a transition procedure;

$F$  is an input function  $F: B \times D \rightarrow \{0, 1\}$ ;

$H$  - output function  $H: D \times H \rightarrow \{0, 1\}$ ;

$M$  is the position marking  $M: B \rightarrow \{0, 1\}$ , and  $M_o$  is the initial marking.

The graphical representation of E-nets is a labelled, bipartite, oriented multigraph.

The functioning of the net consists in the transitions of the kernels from one position to another. Five basic elementary type transitions have been defined for E-nets. The logic of operation of the individual transitions is specified by guidelines for the allowed changes of core locations:

- T-type transition movement of cores  $\{1, 0\} \rightarrow \{0, 1\}$ ;

- Fe-type transition a fork -  $\{1, 0, 0\} \rightarrow \{0, 1, 1\}$ ;

- Je (union) type transition -  $\{1, 1, 0\} \rightarrow \{0, 0, 1\}$ ;

- Transition of type Xe (controlled logic connection)

$\{0, 1, 0, 0\} \rightarrow \{0, 0, 1, 0\}$ ,

$\{0, 1, 0, 1\} \rightarrow \{0, 0, 1, 1\}$ ,

$\{1, 1, 0, 0\} \rightarrow \{0, 0, 0, 1\}$ ,

$\{1, 1, 1, 0\} \rightarrow \{0, 0, 1, 1\}$ ;

- Transition of type Ye (priority logic connection)

$\{0, 1, 1, 0\} \rightarrow \{0, 0, 1, 1\}$ ,

$\{0, 1, 0, 0\} \rightarrow \{0, 0, 0, 1\}$ ,

$\{0, 0, 1, 0\} \rightarrow \{0, 0, 0, 1\}$ ,

$\{1, 1, 1, 0\} \rightarrow \{0, 1, 0, 1\}$ ,

$\{1, 1, 0, 0\} \rightarrow \{0, 0, 0, 1\}$ ,

$\{1, 0, 1, 0\} \rightarrow \{0, 0, 0, 1\}$ .

### III. RESULTS AND DISCUSSION

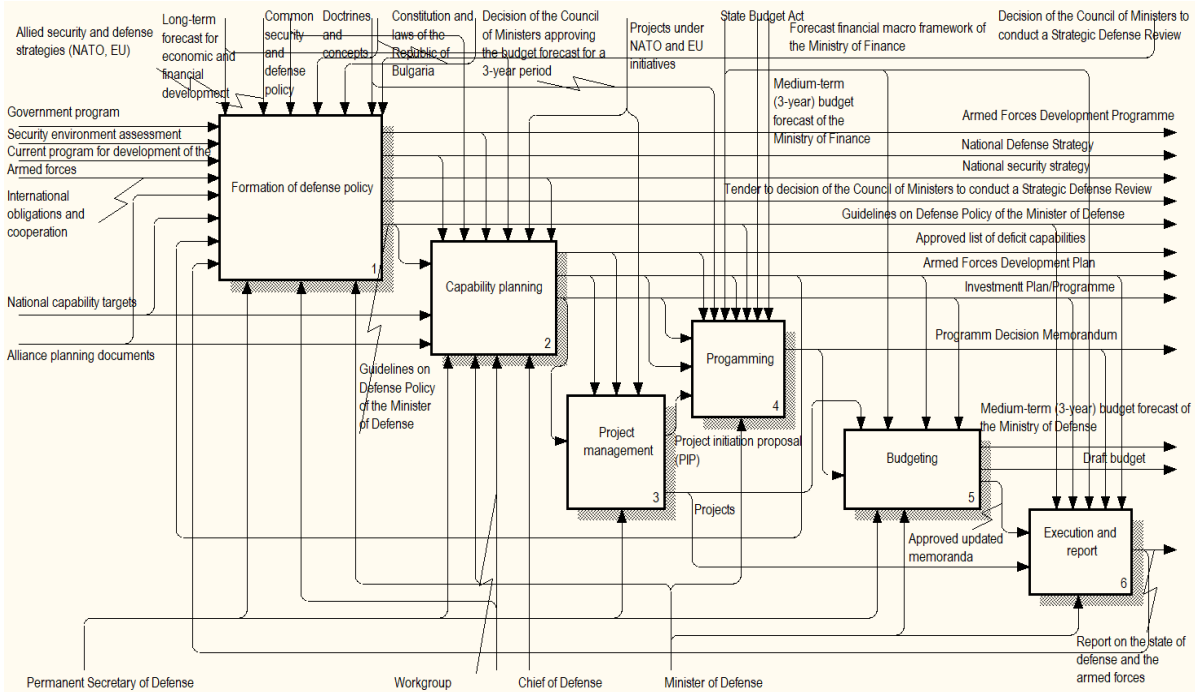
Fig. 1. To-Be model of capability-based defence planning processes

#### 1. ANALYSIS OF THE EXISTING (AS-IS) DEFENCE PLANNING MODEL IN THE AF

The capability-based defence planning process is the main tool to be used in today's security environment, characterized by extreme dynamism, blurring of the boundaries between internal and external security, and an expanding spectrum of hybrid threats [1]. The aim of this process is to protect and promote national interests by building, maintaining and employing defence capabilities adequate to the security environment and by building

2. VERIFICATION OF THE ADEQUACY, COMPLETENESS AND INCONSISTENCY OF THE FORMED (TO-BE) MODEL OF THE DEFENCE PLANNING SYSTEM

The basic requirement for any model is to have the following characteristics: 1) simplicity; 2) adequacy; 3) non-inconsistency; 4) completeness; 5) reliability; 6) flexibility; 7) manageability; 8) constructability; and 9) invariance [2].



interoperable modern armed forces with a unified command and control system in peacetime and in crises.

Since 2012, the Ministry of Defence and the Bulgarian Army have used the capability-based defence planning process as a planning mechanism. A methodological guide has been developed for the implementation of this approach. The realities of the security environment have required a review and update of this document. A comprehensive analysis of the existing defence planning model has been made. The main conclusions of the analysis are that the activity model of the planning process is inconsistent, incomplete and does not correspond to the current defence management system. There is a need to create a new, updated planning model that should: 1) conform to current regulatory and legislative requirements; 2) capture the overall design and dynamics of the system and operating environment; 3) be relevant to the organization's strategic plans; and 4) enable change and transformation activities.

To resolve the identified weaknesses, the model has been refined into an advanced (To-Be) state model to integrate and reflect all major functional and systems perspectives of defence management.

The advanced (To-Be) activity model is depicted in Fig. 1 [1].

The proving of the main characteristics of the To-Be model adequacy, non-inconsistency, completeness, constructability and invariance was done using the described methods.

2.1. E-net model

Based on the IDEF0 activity diagrams in Fig. 1, an E-net interaction model is built (Fig. 2).

To demonstrate the method, only the basic E-net model A0 of the system will be explored. Due to the large size of evidence, the remaining subnetworks are not the subject of this paper. A validation of the overall E-net model, with a complete decomposition of the activities, was accomplished using the Visual Object Net++ Evaluation Version 2.0.

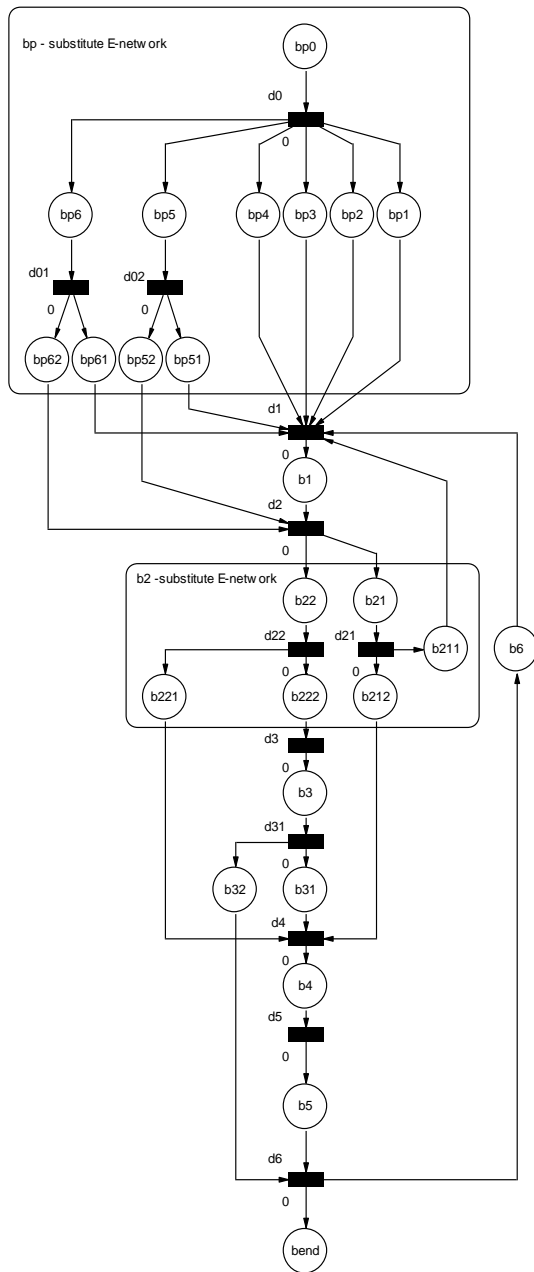


Fig. 2. E-net model of the To-Be A0 model for capability-based defence planning process

When using E-net to model systems and processes, it is possible to use substitute E-net to simplify elementary transitions and positions [5, 6]. In Fig. 2, the macro positions bp and b2 are surrogate E-net as follows:

- bp - substitution E-net with the following positions:
- bp1 - Government program;
- bp2 - Security environment assessment;
- bp3 - Current program for development of the Armed forces;
- bp4 - International obligations and cooperation;
- bp5 (bp51;bp52) - National capability targets;
- bp6 (bp61;bp62) - Alliance planning documents.
- b2 - Substitute E-net with the following headings:
- b21 (b211;b212) - Armed Forces Development Plan;
- b22 (b221;b222) - Investment Plan-Programme.

After the refinements, the E-net model in Fig. 2 obtains the simplified form presented in Fig. 3.

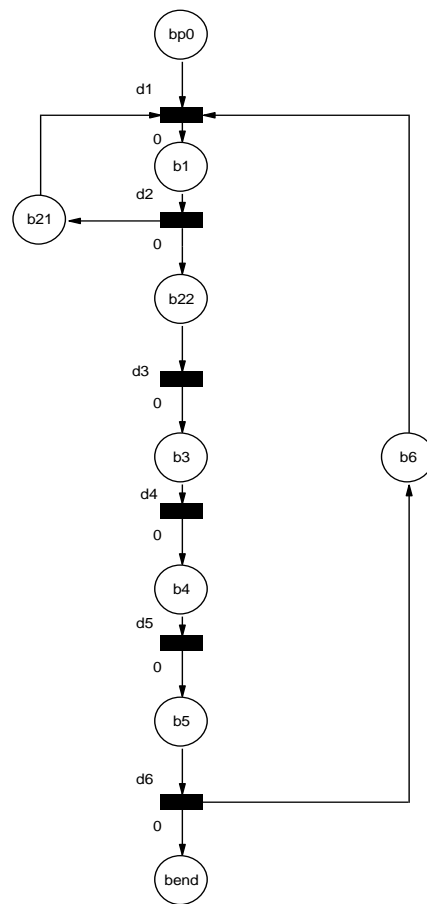


Fig. 3. Simplified E-net model E\_A0

For E-net interaction model E\_A0 the following is defined:

The E\_A0 model is an E-net:

E\_A0 (Bp,B,Br,D,F,H,M0),

Where: Bp = {bp} is set of input positions,

B = {b1, b2, b3, b4, b5, b6, bend} is a set of the following states:

- b1 - Guidelines on Defence Policy of the Minister of Defence;
- b22 - Investment Plan-Programme;
- b21 - Armed forces development plan;
- b3 - Projects;
- b4 - Program Decisions Memorandum;
- b5 - Approved updated memoranda;
- b6 - Report on the state of defence and the armed forces.

Br = {∅}, set of control states;

D = {d1, d2, d3, d4, d5, d6}, set of transitions, where:

d1 - Formation of defence policy;

d2 - Capability planning;

d3 - Project Management;

d4 - Programming;

d5 - Budgeting;

d6 - Execution and report.

F: D∞ B∞, Bp∞, Br∞, (F is a finite set of the input functions F: D∞ B∞, Bp∞, Br∞)

F(d1) = {bp0; b21; b6}, F(d4) = {b3},

F(d2) = {b1}, F(d5) = {b4},

F(d3) = {b2}, F(d6) = {b5}.

H: D∞ B∞, (H is a finite set of output functions D∞ B∞)

$H(d1) = \{b1\}$ ,  $H(d4) = \{b4\}$ ,  
 $H(d2) = \{b2; b21\}$ ,  $H(d5) = \{b5\}$ ,  
 $H(d3) = \{b3\}$ ,  $H(d6) = \{b6; bend\}$ .  
 M0 - initial marking;

$M0 = (1, 0, 0, 1, 0, 0, 0, 1)$ , i.e. there is one core at positions bp, b21 and b6.

The core at position bp occurs when the loop starts and moves to the next position when a transition is executed, and the cores at positions b21 and b6 occur after the initial loop of the process is completed.

The core movement through transitions is shown in Table 1.

TABLE 1 CORE MOTION IN E-NET MODEL E\_A0

Transition	Name	Core motion
d1	Formation of defence policy	1,1,1,0→0,0,0,1
d2	Capability planning	1,0,0→0,1,1
d3	Project Management	1,0→0,1
d4	Programming	1,0→0,1
d5	Budgeting	1,0→0,1
d6	Execution and report	1,1,0→0,1,1

Five basic elementary transition types have been defined for E-net. The logic of operation of the individual transitions is specified by guidelines for the allowed shifts of core locations. In this case, we observed transitions of type Je - a union of cores  $\{1,1,1,0\} \rightarrow \{0,0,0,1\}$ , type Te - a movement of cores  $\{1,0\} \rightarrow \{0,1\}$ , type Fe - a fork  $\{1,0,0\} \rightarrow \{0,1,1\}$  and  $\{1,1,0\} \rightarrow \{0,1,1\}$ .

The relationship between the input F and output H functions of the E-net model is shown in Fig. 3.

Conclusion: When the transitions and reachability of the states of the E-net model E\_A0 are checked, it turns out that all the states are reachable, which means that the presented model is adequate.

## 2.2. Algorithm of E-net model E\_A0

The action algorithm of the process in Fig. 3 is described using a graph diagram. The process primitives of the activity diagram are as follows:

- Start process - primitive (Start);
- Formation of defence policy - primitive (Def\_Pol);
- Capability planning - primitive (Cap\_Plann);
- Project management - primitive (Proj\_Manag);
- Programming - primitive (Progg);
- Budgeting - primitive (Budg);
- Execution and report - primitive (Exec\_Rep);
- Process ending - primitive (End).

The graph schema of the algorithm takes the form of Fig. 4.

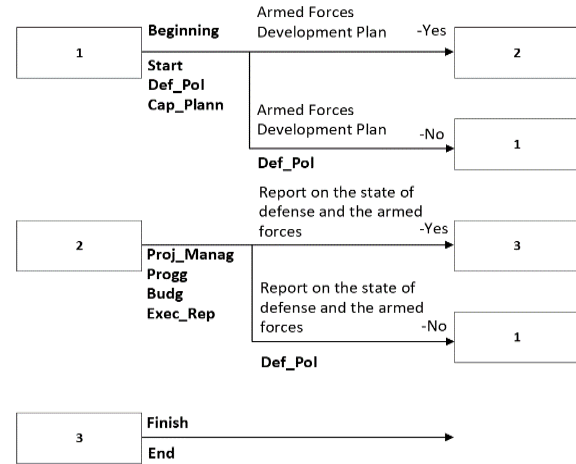


Fig. 4. Graph schema of the algorithm

Statement 1: The operational algorithm of the capability-based defence planning model is complete and non-inconsistent.

Proof: The matrix diagram of the algorithm shown in Table 3 is used to verify Statement 1. The correlation between the primitives and operators of the matrix scheme of the algorithm is presented in Table 2.

TABLE 2 CORRELATION BETWEEN PRIMITIVES AND OPERATORS

Primitives	Start	Def_Pol	Cap_Plann	Proj_Manag
Operators	B <sub>0</sub>	B <sub>1</sub>	B <sub>2</sub>	B <sub>3</sub>
Primitives	Progg	Budg	Exec_Rep	End
Operators	B <sub>4</sub>	B <sub>5</sub>	B <sub>6</sub>	B <sub>end</sub>

Logical conditions:

- p1 - Armed Forces Development Plan (Yes);
- p2 - Report on the state of defence and the armed forces (Yes).

The matrix scheme of the algorithm has the form depicted in Table 3.

TABLE 3 MATRIX DIAGRAM OF THE ALGORITHM

	B <sub>1</sub>	B <sub>2</sub>	B <sub>3</sub>	B <sub>4</sub>	B <sub>5</sub>	B <sub>6</sub>	B <sub>end</sub>
B <sub>0</sub>	1						
B <sub>1</sub>		1					
B <sub>2</sub>	$\bar{p}_1$		p1				
B <sub>3</sub>				1			
B <sub>4</sub>					1		
B <sub>5</sub>		$\bar{p}_2$				p2	
B <sub>6</sub>							1

According to E. Piil the matrix scheme of the algorithm possesses characteristic features that allow to check such important properties of the algorithm as the completeness and non-inconsistency conditions. The completeness condition is met when the disjunction of all elements of a row is equal to 1, and the non-inconsistency condition is met when the conjunction of any two elements of a row is equal to 0 [7].

From the matrix diagram of the algorithm for E-net model E\_A0, it is proved that the model algorithm is complete because the disjunction of all elements in each row is 1 and non-inconsistent because the conjunction of any two elements in each row is 0.

It follows from the proofs that, proposed process model for capability-based defence planning is

constructive and invariant, making it suitable for defining a program application architecture. The model is adequate, complete and non-inconsistent and this ensures its workability in practical implementation.

By analogy, the proofs are applied to all sub-networks of the To-Be model of the capability-based defence planning system.

#### IV. CONCLUSION

The presented revised model of the defence planning process has been adopted as the main methodology for the Strategic Defence Review of the Ministry of Defence and the Bulgarian Army from 2019-2021. The implementation of the model, in practice, occurred through the adopted "Capability-based defence planning guidance-2019" [1]. It was developed for the purpose of the Review and was promulgated by order of the Minister of Defence of the Republic of Moldova. Bulgaria.

The Defence Review validates the updated capability-based defence planning model in practice. It has proven to be a workable tool with a practical application. All the activities of the review have been performed according to the described model, where national strategic objectives are translated into military objectives, possible operations and tasks, and these in turn into forces and capabilities needed to perform these tasks in operations.

#### 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 [11]

the Development of Scientific Research 2017-2030, adopted by Decision of the Council of Ministers No. 731 of 21 October 2021.

#### REFERENCES

- [1] Capability-based defence planning guidance, Mar. 22, 2019. [Online], Available: <https://www.academia.edu/43287181/%D0%A0%D0%AA%D0%9A%D0%9E%D0%92%D0%9E%D0%94%D0%A1%D0%A2%D0%92%D0%9E%D0%97%D0%90%D0%9F%D0%9B%D0%90%D0%9D%D0%98%D0%A0%D0%90%D0%9D%D0%95%D0%9D%D0%90%D0%9E%D0%A2%D0%91%D0%A0%D0%90%D0%9D%D0%90%D0%A2%D0%90%D0%91%D0%90%D0%97%D0%98%D0%A0%D0%90%D0%9D%D0%9E%D0%9D%D0%90%D0%A1%D0%9F%D0%9E%D0%A1%D0%9E%D0%91%D0%9D%D0%9E%D0%A1%D0%A2%D0%98> [Accessed April 05, 2024].
- [2] R. Romanski, "Computer modelling", Technical University Press, Sofia 2002.
- [3] V. Celkov, Models of secure interactions in computer systems and networks, "About letters", Sofia, 2008, ISBN 978-954-8887-45-8.
- [4] 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.
- [5] G. J. Nutt, and J. D. Noe, Some Evaluation Net Macro Structures, Computer Science Group, Univ. Washington, Seattle, TR 73-01-07, 1973.
- [6] G. J. Nutt, The Formulation and Application of Evaluation Nets, Computer Science Group, Univ. Washington, Seattle, TR 72-07-02, 1972.
- [7] E. Piil, On the relation between the language of logic algorithm schemes and Petri nets, Information Network Control Systems, Nauka, Moscow, 1983.
- [8] R. Barker, CASE Method: Tasks and Deliverables, Addison-Wesley, 1990.
- [9] P. Nakov, Fundamentals of Computer Algorithms, "TopTeam Co.", Sofia 1998.
- [10] K. Boyanov, Distributed control of weak connected systems. Technika, Sofia, 1989.

# A Risk-Based Customs Control System in Free Zones

**Normunds Rudzītis**  
Riga Technical University  
Riga, Latvia  
[Normunds.Rudzitis@rtu.lv](mailto:Normunds.Rudzitis@rtu.lv)

**Aldis Čevērs**  
Riga Technical University  
Riga, Latvia  
[Aldis.Cevers@rtu.lv](mailto:Aldis.Cevers@rtu.lv)

**Dana Drubiņa**  
Riga Technical University  
Riga, Latvia  
[Dana.Drubina@edu.rtu.lv](mailto:Dana.Drubina@edu.rtu.lv)

**Sandra Karkliņa-Admine**  
Riga Technical University  
Latvia  
[Sandra.Karklina-Admine@edu.rtu.lv](mailto:Sandra.Karklina-Admine@edu.rtu.lv)

**Abstract.** To support business and promote global trade, the country creates special territories and free zones. Free zones provide entrepreneurs with benefits such as fiscal reliefs, easier access to various resources, and simplified movement of goods, but at the same time create an environment where there are risks of unscrupulous activities. Several studies have concluded that the simplified control of free zone companies and goods implemented by customs authorities poses a high risk of smuggling, violations of intellectual property rights, as well as money laundering. In their research, the authors propose a free zone control model, in which customs risk mitigation measures can be implemented by providing targeted customs control solutions and at the same time without creating additional burdens for entrepreneurs, ensuring fast cargo throughput and increasing the security of international supply chains.

**Keywords:** Control model, customs control, free zones, risks.

## I. INTRODUCTION

Both in the European Union and in other parts of the world, ways to support business and to make global trade faster, more convenient, and more economically profitable are constantly being sought. One of the ways is free zones, which have become especially popular in recent decades, as evidenced by the data on almost 5400 free zones, of which more than a thousand have been created in the last ten years, and this number is expected to increase in the future [1].

Free zones provide entrepreneurs with various tax and customs tariff reliefs, favorable terms for access to land, permits, licenses, employment, administrative facilitation,

and infrastructure support. By taking advantage of these benefits, entrepreneurs are expected to create new jobs, boost exports, diversify the economy, and increase production volumes [1].

However, the benefits and reliefs provided by free zones are also attractive to entrepreneurs who want to carry out illegal circulation of goods and funds. The 47th Research Paper of the World Customs Organization (WCO) expresses the opinion that the control of free zone companies and the goods implemented by customs authorities have been eased, creating a high risk of smuggling, violations of intellectual property rights, as well as money laundering [2].

Free zones can be characterized as "growth poles", which attract foreign direct investment (FDI), thus promoting the economic development of countries and regions. The main advantage of attracting investment is a lower level of bureaucracy [3]. Free zones are one of the production models and to increase production efficiency, it needs an efficient transportation and customs clearance system, which is the reason why free zones located in ports have become the main choice for foreign investment. The characteristic features of free zones are high trade liberalization and internationality, which especially attract foreign investments [4].

On the other hand, other authors take a critical look at free zones and the opportunities and benefits they offer in their research. The offshore space in which free zones operate helps to obscure beneficial owners and illicit trade practices, which hamper authorities' efforts to track money flows and collect taxes [5]. There is also an opinion that the

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8235>

© 2024 Normunds Rudzītis, Aldis Čevērs, Dana Drubiņa, Sandra Karkliņa-Admine.

Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)



model in which free ports operate discourages capital mobility – goods (assets) can be in transit and stored in the free zone for an unlimited time, and they can be sold and moved without being exported or taxed [6]. The purpose of the study is to identify the main security and customs risks of supply chains in free zones, to identify the regulatory framework that ensures customs to manage the possible identified risks, and to provide a solution for monitoring and controlling the operation of free zones. .

## II. MATERIALS AND METHODS

### A. Literature review

The customs and tax reliefs available in free zones attract not only honest entrepreneurs but also players that want to use free zones for illegal activities and profit from them. According to the regulatory regulations of the European Union, it is not necessary to submit a customs declaration for goods in the free zone, so unlike other procedures for storing goods, entrepreneurs do not need to provide a guarantee for goods stored in the free zone [7]. According to the authors, this is one of the most important reliefs, because the financial resources available to the entrepreneurs are not reduced in case of long storage of goods. However, in case of illegal release of goods into free circulation, there is no guarantee for covering the tax debt, and as a result of insufficient information about the goods, there are limited opportunities to determine the value of the goods to calculate the customs debt.

Illicit trade is mainly carried out where there is a weak monitoring system, resulting either from a lack of capacity or overly eased monitoring conditions. In free zones, customs control is mainly carried out based on the information available in the accompanying documents of the goods [8]. The greatest risk occurs when goods are transited or transhipped through free zones, as it is easier to hide the origin or destination of the goods, creating both fiscal risks and threats to public safety and security [3].

The "GRYPHON II" operation implemented in 2016 also shows the vulnerability of free zones to illegal trade. As part of the operation, shipments of tobacco products were especially monitored and more than 700 million cigarettes, almost 300 thousand cigars, and 250 tons of other tobacco products were seized. This operation confirmed that the free zones are being used for the illegal trade of tobacco products, as there were reports of shipments disappearing during transit between the various free zones [9].

Free zones have been established in Latvian ports and their main risks are smuggling, movement of counterfeit goods, violations of the CITES convention, and tax evasion. The number of cases of cigarette and drugs smuggling tends to increase, as shown in Fig.1 by the number of seizures made by the State Revenue Service (SRS) Customs Board in ports in the period from 2020 to 2023.

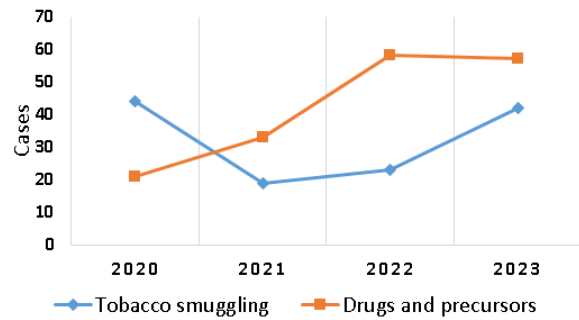


Fig. 1 The number of seizures made by the SRS Customs Board in the period from 2020 to 2023.

There is a risk in the production and distribution of counterfeit goods in free zones. The International Chamber of Commerce (ICC) is critical of free zones, but at the same time points out that most of the free zones act as a tool that promotes international trade and national development. One of the reasons why the illegal trade in counterfeit goods has increased in free zones is that the development of standards, monitoring, and regulations governing the operation of free zones has been slower than the development of these zones [10].

A study conducted in 2018 found that the existence of even one free zone significantly increases the export value of counterfeit and pirated goods from a given economy. There is a direct correlation between the size of free zones, the value of exports, the number of companies and employees existing in them, the volume of investments, and the volume of circulation of goods that violate intellectual property rights. Considering other influencing factors, such as the level of economic development, the fight against corruption, and general trade volumes, it can be argued that free zones are exposed to the risks of moving goods that violate intellectual property rights and are used for the implementation of illegal activities [11]. The share of counterfeit goods from economies with the 20 largest free zones is twice that of economies without any free zones [12].

The risks associated with the use of free zones for money laundering and terrorist financing have also been specially studied. The Financial Action Task Force (FATF) concluded in a 2010 study that trade-based money laundering is one of the most common methods used by organizations to launder proceeds of crime. Using complex schemes, invoices are issued with a reduced or increased value of goods, which is easier to implement in the free zone. Fictitious shipments are made, false value and quantity of goods are applied, one form of fraud is the issuing of multiple invoices for goods to justify an increase in value and the transfer of goods to another jurisdiction. The most common offenses in which free zones can be used to launder proceeds of crime are smuggling, illegal drug trade, membership in organized crime groups, fraud, as well as the distribution of counterfeit goods [13]. The environment of free zones is good for hiding and making it as difficult as possible to identify the real beneficiary of illegal profits and the origin of those profits, for example when dealing in goods stored in free zones such as works of art. The buyer can store the works of art purchased by illegal means in the free zone, naming the cargo agent as responsible and not revealing the true owner of the goods [14].

Between 2011 and 2018, the Customs Enforcement Network (CEN), established by the WCO, received reports from 48 countries of more than 600 seizures related to free zones. The structure of confiscation cases is shown in Fig.2.

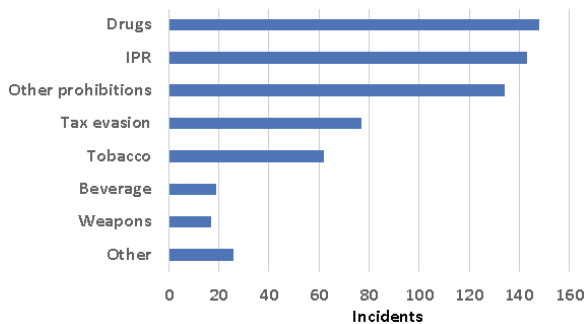


Fig. 2 Structure of seizures in free zones in the period from 2011 to 2018 [12].

The structure of seizures demonstrates the main groups of risks – cigarette and drug smuggling, intellectual property violations, and tax evasion. Violations detected in free zones are global. The country of dispatch of the confiscated goods and the country where the violation was detected may differ or be from different regions, and there may also be situations where countries belong to the same region. For example, the share of counterfeit goods from economies with the 20 largest free zones is twice that of economies without any free zones [12].

### B. General analysis

One of the factors that make free zones more susceptible to illegal activities is the lack of international standards governing the movement of goods through free zones in transit, as the monitoring of goods in transit usually becomes a secondary objective [15]. International regulations that have an impact on global trade do not always clearly formulate requirements for goods in free zones [2]. It should be noted that agreements containing clear requirements for free zones aim to reduce the risks of illegal drug trade, tobacco smuggling, and intellectual property rights in free zones. The authors of the paper believe that it would be particularly important to include specific provisions for free zones in the legislation that regulates the other previously identified groups of existing risks, such as the illegal movement of fauna and flora specimens (CITES) and the use of cultural objects for money laundering, which is one of the frequently described methods used for money laundering in free zones.

One of the most important legal acts in the field of customs is the International Convention on Simplification and Harmonization of Customs Procedures [16]. Chapter Two of Special Annex D of the Revised Kyoto Convention contains 21 standards and recommended practices that define the principles of the zones' operation. There are cases where the concept used in the Revised Kyoto Convention, that free zones are considered to be outside the customs territory, is misinterpreted and leads to the concept of "extraterritorial free zone", which has a reduced involvement of customs services in the monitoring of goods and eased customs control measures are applied [2]. Free zones are established in the geographical territory of countries, but the government has defined them as structures outside the normal customs regime [5].

The revised Kyoto Convention stipulates that customs services can control goods located in free zones at any time [16], but there are also cases where this norm is not implemented in reality, for example, customs officers cannot enter the territory of the free zone without prior approval. The customs cannot stop the operation of the free zone even if the customs have evidence of smuggling activities, the customs authorities of individual countries have the right to check the cargo only at the moment of its import or export, data on the movement of cargo in free zones are not submitted, as a result of which certain important information is not available to customs administrations and customs control is limited [2]. Existing standards, monitoring, and other controls for free zones have expanded, but have not always kept pace with the growth in the number of companies and the volume of illegal trade in goods and services. Competent state authorities do not always have timely physical access to the premises, there are difficulties in obtaining information on the activities of companies registered in the free zone with goods and on the ownership of goods that are moved in transit, manufactured, or assembled in free zones, even in cases where international standards require it [17].

In Latvia, the physical access of the customs service to the free zones is ensured, however, however, access to real-time data on goods imported, exported and stored in free zones, as well as the sender and receiver of the goods, does not provide opportunities for automated risk analysis, as IT systems are not integrated into a single system. Information about the real sender and receiver is not always specified in the cargo manifest, and accompanying documents are not always included in the application for moving or unloading goods. It should be noted that the submission of summary declarations on imported and planned exported goods is an essential source of information for risk analysis, however, it should also be noted that the information included in the summary declarations is aimed at assessing security risks, while the information required for fiscal risk analysis is insufficient. The authors conclude that the Revised Kyoto Convention has an insufficient set of standards and recommended practices that apply to the identified risks of free zones and directly determine the requirements for the effective organization of customs control over goods stored in free zones. The Convention also does not include the recommendations put forward by the WCO on the integration of IT systems, the involvement of customs authorities in the process of creating free zones, or the promotion of the use of Authorized Economic Operator (AEO) status [16].

As a member state of the European Union, Latvia is bound by the regulatory framework of the European Union and the national legislation must be based on the legal acts of this framework. The movement and accounting of goods in Latvia is regulated by Cabinet of Ministers Regulation No. 500 of August 22, 2017 "Regulations of Customs Warehouses, Temporary Storage and Free Zones", as well as regulations incorporated in the Customs Law, which delegate the Cabinet of Ministers to determine the procedure for recording stored, processed, sold or purchased non-EU goods in the free zone.

Taking into account the peculiarities of the procedure, the Union Customs Code (UCC) [7] provides that it is necessary to record the goods in a manner approved by the

customs services, and the records must also include information that allows the customs services to monitor the relevant procedure by identifying the goods, determining their customs status and implementing the transfer [7], however, the regulatory acts of the European Union do not specify more detailed requirements on how goods must be recorded, as well as certain requirements to provide customs with electronic access to company accounting systems for automated risk assessment.

Commission Delegated Regulation 2015/2446 of July 28, 2015, supplementing Regulation of the European Parliament and Council (EU) no. 952/2013 regarding the detailed regulations that apply to some provisions of the UCC (hereinafter referred to as the Delegated Regulation) provide for several data elements that must be included when accounting for goods, and the national regulation specifies this. However, at the national level, the information circulation system established in the regulatory framework stipulates that the accounting and identification of goods is ensured by the person in whose free zone non-EU goods are stored, processed, sold, or bought, which means that the holder of the free zone permit is responsible [18], and the record is not required from the user of the procedure or other persons who carry out the relevant operations with the goods as defined in the UCC [9], so it could be said that the national regulation contains lighter requirements. The authors believe that the elements of data indicated in the inventory are only slightly different from those that need to be included in the inventory of goods in the customs warehouse, which in turn shows that the existing regulation determines the need to provide a lot of information about goods in free zones. It is not sufficient for customs control, so the condition of providing a customs declaration would not lead to drastic changes in the formalities when applying the special procedure of "storage in a free zone".

The existing regulatory framework allows goods to be processed without changing, or in some cases changing, the eight-digit combined nomenclature code when applying storage in the free zone. A deeper analysis of the permitted actions concludes that, for example, after adding goods accessories, changing packaging, and cutting goods (specifically applicable to general cargo), tracking and controlling goods is practically impossible. The regulation of the UCC stipulates that the customs services have the right to prohibit from carrying out activities in the free zone persons who do not provide the necessary guarantees that the customs regulations will be observed [7], unfortunately, the national regulation only provides for evaluating whether the type of accounting of goods introduced by the free zone companies meets the requirements [18].

In Table 1, the authors of the study have collected data on the compliance of the regulatory framework contained in legal acts with the determined risk mitigation measures.

TABLE 1 REQUIREMENTS FOR RISK MITIGATION MEASURES IN FREE ZONES [16], [7], [18]

	The Regulatory Act	Revised Kioto Convention	Union Customs Code	National Regulation in Latvia
Risk mitigation measures in free zones (FZ)	Definition of FZ as part of the customs territory	-	+	-
	Ensuring customs control in free zones	+	+	-
	Control of incoming outgoing vehicles	-	+	-
	Requirements for AEO status	-	+	-
	Providing data about companies	-	-	-
	Customs checks on entrepreneurs in FZ	-	+	-
	Customs provides company training and information	-	-	-
	Involvement of customs in the planning process of FZ	+	/	-
	Need to coordinate of any operations with goods in FZ	/	/	/
	Submission of a simplified declarations	-	-	-
	Integration of IT systems in FZ	-	-	+

One of the shortcomings is the low level of involvement of customs authorities both in determining the regulation of free zones and in planning operations. It is explained that such a situation has arisen because the creation of free zones is primarily based on economic and industrial importance, and ministries play a key role in the implementation of policies, the creation of free zones, and the approval of entrepreneurs. According to the survey data, approximately 40% of the customs administrations of the member states are not involved in the process of creating free zones and in evaluating the applications of entrepreneurs who want to operate in the free zones [2]. Customs implements limited cooperation with the private sector as well [15]. Controls of free zones are often random rather than based on risk analysis [13].

The lack of reliable monitoring of the users and administrators of free zones is mentioned as an additional risk factor. Information on the monitoring of the security-related activity of the administrators of free zones, which in some cases is not even there at all, is not made public, so the control is not considered sufficiently effective in cases where the activity of a specific zone could have a bad impact on the country's reputation [15]. Both the reputation and the security of international supply chains depend on the monitoring of free zones [3]. There is no substantive obligation on free zone entrepreneurs to ensure that they do not facilitate illegal trade by acting on behalf of third parties [15]. On the other hand, reduced monitoring can be described as an advantage, as it creates a private business environment for more successful international competition [5].

The operation of free zones is aimed at liberalization or reduction of controls, including simplification of customs procedures. These risks are not always considered in the free zone planning process [15]. In recent years, the awareness of the risks existing in free zones has grown significantly, however, these risks are not considered because they are judged to be insignificant in relation to the potential economic benefits of the countries.

In free zones, there are risks associated with the circulation of certain goods that are particularly vulnerable due to their value, size, high tariff rate, volume of trade, and potential violations of intellectual property rights, such as

cigarettes, alcohol, luxury goods, and electronics [13]. In Latvia, there are special regulations regarding excise goods, for example, for moving such goods from one free zone to another, it is necessary to draw up a transit declaration. The authors believe that a significant risk-increasing factor is the possibility of performing various actions in free zones with any type of goods, repackaging, dividing, and changing the label, thereby significantly reducing or even losing the ability to track them. If the traceability of goods is lost, then entrepreneurs have ample opportunities to carry out crimes, for example, forge documents, exchange goods, make fictitious transactions

A significant disadvantage in free zones is also the lack of coordination of information systems, most often there are separate and different systems for entrepreneurs and customs [13]. Customs risk management is essentially data-driven, and in this case, the lack of information on cargo movement and company's operations in free zones hinders risk analysis [2]. The International Chamber of Commerce, on the other hand, believes that the lack of integration of information systems may not be a significant problem if customs are provided with access to the systems of free zone companies so that reusable data can be exchanged [19].

Based on the previously analyzed information, a total of seven risk-promoting factors in free zones can be distinguished, however, only 4 factors are those that can be directly acted upon by the customs authorities (see Fig.3)

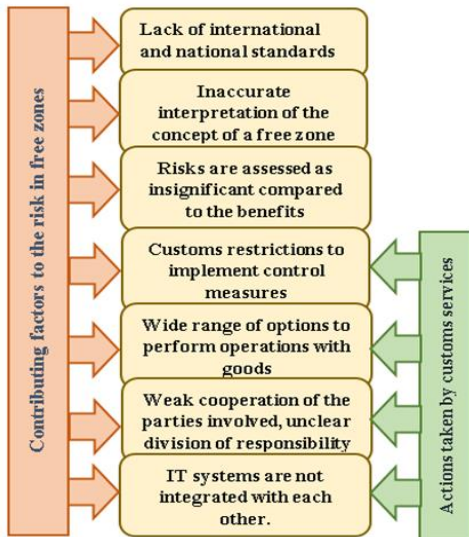


Fig. 3. Contributing factors to the risk in free zones

To develop a safe environment for international trade in free zones, customs authorities need full-fledged legal protection. Although the limited ability of customs services to carry out control measures in free zones is closely related to, for example, the lack of international standards, weak cooperation with other monitoring organizations, opportunities for entrepreneurs to take advantage of the reliefs in free zones through regular document controls and physical inspections, as well as the provision of a free zone the resources necessary for monitoring, customs services can increase their ability to perform adequate monitoring of free zones, as well as reduce the negative impact of the wide range of permitted operations with goods in the free zone . One of the most important risk-promoting factors is

the lack of integration of information systems, so customs services need to show initiative to inform about the existing problem and jointly implement measures with the private sector to ensure the flow of information.

### III. RESULTS AND DISCUSSION

Due to the wide distribution of free zones around the world and the regional differences that exist, the practices implemented in the movement and storage of goods in free zones vary. If, for example, in the European Union, thanks to a uniform legal framework, the monitoring of free zones is carried out according to uniform basic principles, then, for example, there may be considerable differences in third countries.

The authors, based on the existing risk-promoting factors in the free zones and the gathered existing risk-mitigating measures, have developed an optimal free zone control model (see Fig. 4). This model is based on four levels, the first of which involves the development of a clear regulatory framework in free zones.

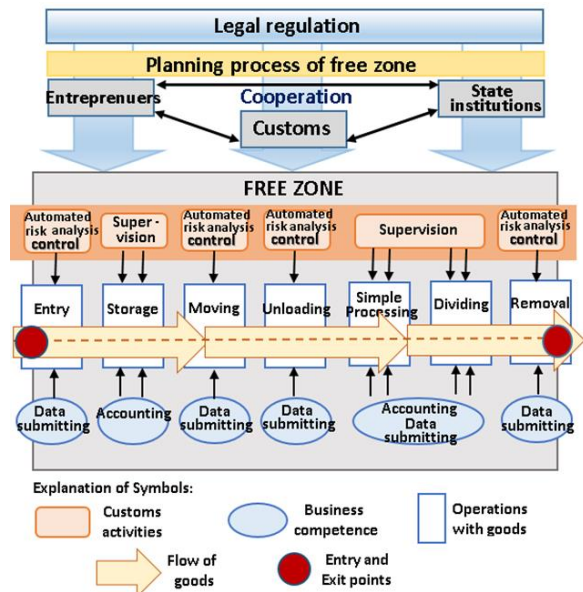


Fig. 4. Free zone control model

It is necessary to develop uniform international requirements that establish that free zones are included in the customs territory of a particular country or union and provide customs authorities with the same powers as in any other part of this territory. Countries should define in their legislation and implement in practice the requirements contained in the standards and recommended practices of Annex D of the Revised Kyoto Convention [16]. State or union-level regulation should provide requirements not only for customs and other state authorities but also for entrepreneurs, clearly defining the rights and obligations of all parties. It is important to establish that the customs authorities have the right to request the data they need to carry out full-fledged control over non-EU goods in the free zone, but the entrepreneurs should provide provisions regarding the possible reliefs and benefits as a result of the systematic fulfillment of these requirements.

The second level determines the involvement of customs services in the planning and development process of free zones as an integral part of the process. It is necessary to assign representatives of the customs service to work in the relevant groups for the planning and development of free zones so that they assess the risks created by the reliefs in relation to the economic benefits created by the free zones. A successful solution for reducing customs risks is to involve in the operation of free zones those entrepreneurs that are recognized by the customs services and have received a certain amount of relief in performing customs clearance activities. For example, in Estonia, the normative regulation stipulates that holders of permits for customs warehouses, temporary storage places, and free zones need a recognized consignee's permit to receive transit cargo transported by road transport, a similar practice is also implemented in the Netherland port of Rotterdam [20]. This practice is recommended in other countries, when planning the attraction of entrepreneurs and the creation of a support program, in cooperation with customs services, creating a favorable environment for successful business.

The Recognized Economic Operator model defined in the SAFE standards [21] has been widely used in many countries around the world. In general, this model of cooperation between entrepreneurs and customs services has been implemented in 98 WCO member states and it increases the security of supply chains and reduces customs risks. Therefore, it is useful to evaluate the possibilities of the certification of Safe Free Zones, based on the AEO concept, the Trade Promotion Agreement, and the Code of Clean Free Trade Zones, which, as recognized by the Klaipeda Free Economic Zone, emphasizes better cooperation obligations between the parties involved and improves the image policy of free zones [22]. Before issuing a permit to operate in a free zone, it is necessary to ensure that customs have the opportunity to conduct a risk analysis of companies, avoiding situations where high-risk companies operate in the free zone. The free zone planning process should provide not only the creation of free zones, but also the creation and management of unified infrastructure elements, thus preventing situations where each controlling and monitoring institution creates different infrastructure elements that perform the same functions, and reducing resource consumption.

The third level in the created free zone control model is based on cooperation, where one of the elements is a qualitative exchange of information between entrepreneurs and customs. When creating the flow of information, it is necessary to provide opportunities not only for customs services to perform risk analysis but also for entrepreneurs, because a large part of free zone companies are members of supply chains, for whom it is important to know the risks of their cooperation partners. It is also essential to cooperate in the implementation of various innovations, allowing entrepreneurs to express their opinions on the planned changes. Cooperation between customs and other supervisory authorities should be based on the division of responsibilities and sharing of resources, which, according to the author, is one of the factors promoting development. According to the author,

if one of the recommendations for improving the control of free zones is to provide customs with opportunities to control entry and exit points in free zones, then it is necessary to closely cooperate with organizations responsible for monitoring the territory and persons.

The fourth and most important level is the process of control of goods in free zones, which is based on the provision of information, based on which it is possible to perform a qualitative risk analysis. The main prerequisite is the submission of data necessary for risk analysis before operations with goods: application of the procedure, movement, unloading, and removal from the free zone. The submission of this data must be done electronically, by submitting, for example, the simplified declaration or by entering the relevant information in any other way into the system, so that an automatic risk analysis can be performed. Along with the submission of data, the problem of product traceability would also be addressed, as an identification number is assigned to each shipment. The World Customs Organization proposes a Unique Consignment Reference (UCR) number, which aims to define a general mechanism flexible enough to deal with the most common scenarios occurring in international trade, making the most of existing references of supplier, customer, and transport. Such a reference number allows the information systems of customs and trading parties to cooperate most efficiently and, when properly applied, it also ensures the exchange of data between declarations and manifests [23]. An important element of the control options is the submission of summary declarations when entering and leaving the free zone or moving goods within the free zone. It is also necessary to ensure the monitoring of incoming and outgoing cargo, consumed goods and losses, the traceability of the weight of goods stocks, and the possibility to control the basic data of customs and global trade compiled by the classification, value, and origin of goods, and it is also necessary to define clear requirements and procedures for third-party service providers [24].

One way to ensure automatic data submission and availability to customs is the integration of entrepreneurs and customs information systems, providing the opportunity to submit data to the customs information system, while simultaneously performing an inventory of goods. The monitoring of the inventory of goods should be based on a risk analysis, which can be ensured if the customs have continuous access to the data on the goods registered in the free zones and the operations carried out with them. The implementation of such conditions can be ensured by the condition that companies operating in free zones must comply with the AEO standards, which require the entrepreneur to provide electronic access to accounting data.

#### IV. CONCLUSIONS

Summarizing all the analysis carried out, it can be argued that free zones are unique due to the wide range of advantages they offer, providing the opportunity to attract foreign investment, reducing the tax burden on companies existing in free zones, which contributes to the expansion of companies, the creation of new jobs and the

development of a given country or region. At the same time, reducing the administrative burden in free zones increases the level of risks of illegal goods circulation, which in turn negatively affects the security of supply chains, causes losses to the state budget, creates a negative impact on public health, the surrounding environment, and also threatens the preservation of cultural heritage.

The main factors that hinder the operation of customs control and surveillance system include the lack of resources allocated to customs control, shortcomings in the legal framework and ineffective integration of information systems. These factors limit the establishment of an automated customs risk management system in free zones and restrict the customs authority's capacity to take effective and targeted customs control measures.

Countries should create free zones and use their advantages, but at the same time, they should continuously monitor existing trends and recommendations that would reduce the economic, safety, and security risks associated with the creation of free zones and provide opportunities to implement sufficient customs control and at the same time not create additional burdens for entrepreneurs, maintaining fast cargo throughput and security of international supply chains.

An optimal free zone control model covers the continuous improvement of the regulatory framework at the international, regional, and national levels, ensuring the involvement of customs services in the free zone planning process, using the cooperation of parties operating in free zones, promoting the exchange of information, the distribution of duties and responsibilities, and ensuring that customs service's implement a risk analysis-based monitoring and control of imported, exported, moved and stored goods in free zones.

## REFERENCES

- [1] World Investment Report 2019. Special Economic Zones (2019) [online]. United Nations Conference on Trade and Development . Available at: [https://unctad.org/system/files/official-document/WIR\\_2019\\_CH4.pdf](https://unctad.org/system/files/official-document/WIR_2019_CH4.pdf) [Accessed March 23, 2023]
- [2] Omi, K. (2019). 'Extraterritoriality' of Free Zones: The Necessity for Enhanced Customs Involvement, WCO Research Paper, No. 47, pp. 1-34. Available at: [http://www.wcoomd.org/media/wco/public/global/pdf/topics/research/research-paperseries/47\\_free\\_zones\\_customs\\_involvement\\_omi\\_en.pdf](http://www.wcoomd.org/media/wco/public/global/pdf/topics/research/research-paperseries/47_free_zones_customs_involvement_omi_en.pdf) [Accessed March 29, 2023]
- [3] Polner, M., Kagawa, S. (2018). Addressing challenges related to Customs controls in free zones. WCO news, Vol. 87, pp 75-77. Available at: [https://mag.wcoomd.org/uploads/2018/10/WCO\\_News\\_87.pdf](https://mag.wcoomd.org/uploads/2018/10/WCO_News_87.pdf) [Accessed February 18, 2023]
- [4] Hsu, W.-K.K., Huang, S.-H.S., Huynh, N.T. (2021). An Evaluation Model For Doreign Direct Investment Performance of Free Trade Port Zones. Promet - Traffic – Traffico, Vol. 33(6), pp. 859-870. Available at: <https://traffic.fpz.hr/index.php/PROMTT/article/view/3844/561561980> [Accessed April 6, 2023]
- [5] Gilmour, P.M. (2022) Freeports: Innovative trading hubs or centres for money laundering and tax evasion? Journal of Money Laundering Control, Vol. 25(1), pp. 63-71. Available at: [https://pure.port.ac.uk/ws/portalfiles/portal/25829454/Freeports\\_Post\\_print.PDF](https://pure.port.ac.uk/ws/portalfiles/portal/25829454/Freeports_Post_print.PDF) [Accessed May 18, 2023]
- [6] Schwarzkopf, S., and Backsell, J. I. (2020). The Nomos of the Freeport. Environment and Planning. Society and Space, Vol. 0, pp. 1-19. Available at: <https://doi.org/10.1177/0263775820944523> [Accessed May 12, 2023]
- [7] Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code, 1010.2013, Official Journal of the European Union, Available at: <https://eur-lex.europa.eu/legal-content/ENGL> [Accessed March 11, 2023]
- [8] Holden, C. (2017). Graduated sovereignty and global governance gaps: Special economic zones and the illicit trade in tobacco products, Political Geography, Vol. 59, pp. 72-81. Available at: <https://www.sciencedirect.com/resursi.rtu.lv/science/article/pii/S0962629817300781?via%3Dihub> [Accessed March 24, 2023]
- [9] Millions of cigarettes seized during Operation GRYPHON II (2016) [online]. World Customs Organization webpage [accessed 3 May 2022]. Available at: <http://www.wcoomd.org/en/media/newsroom/2016/july/millions-of-cigarettes-seized-during-operation-gryphon-ii.aspx> [Accessed May 10, 2023]
- [10] ICC Recommendations on Illicit Trade in Free Trade Zones (FTZs) (2017) [online]. ICC Commission on Customs and Trade Facilitation Available at: <https://iccwbo.org/content/uploads/sites/3/2017/12/icc-recommendations-on-illicit-trade-in-free-trade-zones.pdf> [Accessed March 18, 2023]
- [11] Trade in Counterfeit Goods and Free Trade Zones: Evidence from Recent Trends (2018) [online]. OECD Publishing, Paris/EUIPO, Available at: [https://read.oecd-ilibrary.org/trade/trade-in-counterfeit-goods-and-free-trade-zones\\_9789264289550-en#page4](https://read.oecd-ilibrary.org/trade/trade-in-counterfeit-goods-and-free-trade-zones_9789264289550-en#page4) [Accessed March 24, 2023]
- [12] Mapping the Impact of Illicit Trade (2019) [online]. The Transnational Alliance to Combat Illicit Trade (TRACIT) webpage [accessed 6 April 2022]. Available at: [https://unctad.org/system/files/non-official-document/DITC2019\\_TRACIT\\_IllicitTradeandSDGs\\_fullreport\\_en.pdf](https://unctad.org/system/files/non-official-document/DITC2019_TRACIT_IllicitTradeandSDGs_fullreport_en.pdf) [Accessed March 18, 2023]
- [13] Money Laundering Vulnerabilities of Free Trade Zones (2010) [online]. FATF Report, FATF webpage [accessed 27 March 2022]. Available at: <https://www.fatf-gafi.org/media/fatf/documents/reports/ML%20vulnerabilities%20of%20Free%20Trade%20Zones.pdf> [Accessed March 24, 2023]
- [14] Steiner, K., L. (2017). Dealing with Laundering in the Swiss Art Market: New Legislation and its Threat to Honest Traders. Case Western Reserve Journal of International Law, Vol. 49, Issue 1, Article 21, pp. 351-372. Available at: <https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=2515&context=jil> [Accessed May 18, 2023]
- [15] Moiseienko, A., Reid, A., Chase, I. (2020). Improving Governance and Tackling Crime in Free-Trade Zones [online]. The Royal United Services Institute, Available at: <https://rusi.org/explore-our-research/publications/occasional-papers/improving-governance-and-tackling-crime-free-trade-zones> [Accessed May 10, 2023]
- [16] International Convention on the Simplification and Harmonization of Customs Procedures, Revised (2006) [online]. International convention, done at Kyoto on 18 May 1973, revised on 2006, World Customs Organization, Available at: [http://www.wcoomd.org/en/Topics/Facilitation/Instrument%20and%20Tools/Conventions/pf\\_revised\\_kyoto\\_conv/Kyoto\\_New](http://www.wcoomd.org/en/Topics/Facilitation/Instrument%20and%20Tools/Conventions/pf_revised_kyoto_conv/Kyoto_New) [Accessed May 18, 2023]
- [17] Recommendation of the Council on Countering Illicit Trade: Enhancing Transparency in Free Trade Zones (2019) [online]. OECD webpage [accessed 2 February 2022]. Available at: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0454> [Accessed May 18, 2023]
- [18] Regulations of the Cabinet of Ministers of August 22, 2017 No. 500 "Regulations on Customs Warehouses, Temporary Storage and Free Zones" (2017), adopted in Riga on August 22, 2017, Latvijas Vēstnesis, website Likumi.lv. Available:

- <https://likumi.lv/ta/id/293175-muitas-noliktavu-pagaidu-uzglabanas-un-brivo-zonu-noteikumi> [Accessed May 7, 2023]
- [19] Controlling the Zone: Balancing facilitation and control to combat illicit trade in the world's Free Trade Zones (2013). International Chamber of Commerce webpage. Available at: <https://iccwbo.org/content/uploads/sites/3/2016/11/Combating-illicit-trade-in-FTZs-1.pdf> [Accessed May 25, 2023]
- [20] Täpsustavad juhised ajutise ladustamise, tolliladustamise ja vabatsoonis tegutsemise kohta Nr. 58 (2017) [tiešsaiste]. Regulations of the Cabinet of Ministers of the Republic of Estonia, adopted on July 4, 2017, Riigi Teataja website. Available at: <https://www.riigiteataja.ee/akt/115012019008> [Accessed October 17, 2023]
- [21] SAFE Framework of Standards (2021) [online]. World Customs Organization webpage. Available at: <http://www.wcoomd.org//media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/safe-package/safe-framework-of-standards.pdf?la=en> [Accessed February 22, 2023]
- [22] Safe Zone Certification Program by World Free Zones Organization (2021) [online]. World FZO TV YouTube channel [Accessed April 10 2023]. Available at: <https://www.youtube.com/watch?v=nc70hSVo1KA>
- [23] WCO Unique Consignment Reference (UCR) (2004) [online]. World Customs Organization webpage, Available at: <https://www.wcoomd.org/en/topics/facilitation/resources/~media/633F01FC1783462EA9DBDE125AF48834.aspx> [Accessed February 22, 2023]
- [24] ME Customs and Global Trade webinar. Managing Customs for Free Zones and Mainland - Opportunities and Challenges (2021) [online]. Deloitte webpage [accessed 10 April 2022]. Available at: <https://www2.deloitte.com/content/dam/Deloitte/xe/Documents/tax/dme-customs-global-trade-webinar.pdf> [Accessed March 16, 2023]

# *Attitudes of Latvian external border custom officers towards work*

**Vladislavs Sardiko**  
Faculty of Education and  
Management  
Daugavpils University  
Daugavpils, Latvia  
vl.sardiko@gmail.com

**Abstract.** Topicality of the study: It is essential to understand what is important to employees, what their main motivation factors are, and the attitudes towards work. An employee's orientation towards processes, work, money, and results can significantly influence their performance and attitude towards work. The elements of this motivation shape employee's vision of their role in the organization and how they prioritize their responsibilities and goals.

**The aim the study:** To investigate the personal attitudes of Latvia's external border customs employees towards work.

**Methodology:** The main methodology employed in this research was an adopted version of O.Potemkina's questionnaire "Diagnosis of socio-psychological attitudes of a person in the motivational-need sphere". Out of the original 80 questions, 40 questions were selected and used according to the criteria (process, result, work, income).

Additionally, a comprehensive questionnaire was applied to categorize respondents based on various indicators, including marital status, educational level, and gender. This approach facilitated a thorough analysis of the correlations between the primary research questions and different aspects of the respondents' profiles.

**Main findings:** Women are more process-oriented, therefore more work with documents could be delegated to them, but on the other hand, men, being more result-oriented, and they are better positioned for roles in combating smuggling from a management perspective. Education is also of great importance, as it significantly changes the difference in results depending on the level of education.

This approach could be highly beneficial before a job interview as it would reveal the motivation of the potential employee. If financial considerations are the primary motivation for the applicant, it might indicate that such an employee may not work with the customs for an extended period.

**Keywords:** attitudes, custom employees, external border

## I. INTRODUCTION

The aim the study: To investigate the personal attitudes of Latvia's external border customs employees towards work.

The attitude of Latvian external border customs officers towards work is essential in ensuring national security and customs control. These customs officers assume a responsible role in controlling the movement of goods across the border to ensure legal and safe customs operations[1].

One of the main factors influencing the attitude of customs officers is the need to be careful and precise in their daily work. They work with a variety of different situations and groups of people, so it is important to maintain a professional attitude and neutrality. Customs officers are regularly trained on new customs rules and procedures to ensure their knowledge is current and relevant [2]. Therefore, the functions and tasks of customs are variable and depend on both external (political, economic, social and technological) and internal (resources, processes and culture) factors [3].

On the other hand, the attitude of employees also directly affects customer experience and relationships. Although customs officials may experience challenges and tensions, it is important that they maintain a professional attitude and help citizens understand customs procedures.

To demand high efficiency at work from employees, it is necessary to understand the orientation of the employees towards their tasks. It is important to know which aspects of the job bring more pleasure to the employee. The research has novelty, as such research has never been

Print ISSN 1691-5402  
Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8200>

© 2024 Vladislavs Sardiko. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)



conducted before for Latvia's external border customs employees.

## II. MATERIALS AND METHODS

The main methodology employed in this research was an adopted version of O.Potemkina's questionnaire "Diagnosis of socio-psychological attitudes of a person in the motivational-need sphere". Out of the original 80 questions, 40 questions were selected and used according to the criteria (process, result, work, income).

Additionally, a comprehensive questionnaire was employed to categorize respondents based on various indicators, including marital status, educational level, additional income, level of competence, dependents and gender. This approach facilitated a thorough analysis of the correlations between the primary research questions and different aspects of the respondents' profiles.

Respondents - 113 senior customs supervisors working at Latvia's external border (The total number of senior customs supervisors in the State Revenue Service Customs Board is 520, the survey's maximum after selection was 320 senior customs supervisors). The study was conducted from 01.05.2022 to 30.06.2022. Anonymous questionnaires were offered in electronic or paper form.

The obtained results allowed to trace the orientation of employees towards work.

## III. RESULTS AND DISCUSSION

Further the author discusses the results by selecting some variables: gender, marital status, additional income, level of competence.

Research allows to conclude that women play important role in customs, although there is a male predominance [5], not as big as in 2021 according to WCO data, 37 percent of the world's customs employees are women, and 16 percent of senior customs positions are held by women [6]. When working on the external border of Latvia, the work of senior customs supervisors is not divided according to gender, all the necessary tasks that senior customs supervisors must be able to perform, except for work with X-ray equipment, where an employee with a special permit can only work, but such permits are available for both women and men.

However, the author concludes that gender could make a difference in regards to an attitude towards work.

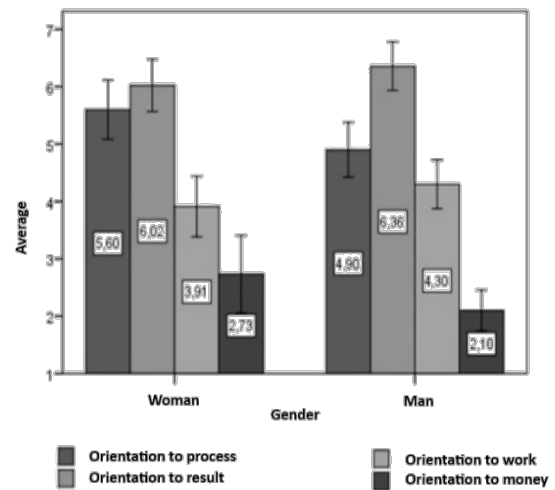


Fig.1. Job orientation breakdown by gender

Fig. 1 shows the distribution of the results obtained according to gender. We see how the common picture is the same and the greater emphases is placed on the result, rather than on the process, on the work and the last towards money. There are also visible differences of attitudes in gender variable. Female representatives are more inclined to process and money unlike men, while men are more inclined to work and result.

The results obtained as a result of an independent sample T-test indicate (Table I) that between men and women, there is a significant difference in orientation towards the process among the senior custom supervisors. For women, this aspect is more important.

TABLE I JOB ORIENTATION ACCORDING TO GENDER VARIABLE (INDEPENDENT SAMPLES TEST)

	t-test for Equality of Means		
	t	df	Sig. (2-tailed)
Orientation towards process	1,930	113	,049
Orientation towards result	-1,043	113	,299
Orientation towards work	-1,149	113	,253
Orientation towards money	1,814	113	,072

As for the next question, the author can conclude that marital status can also be important. Employees' orientation towards money could increase for married respondents.

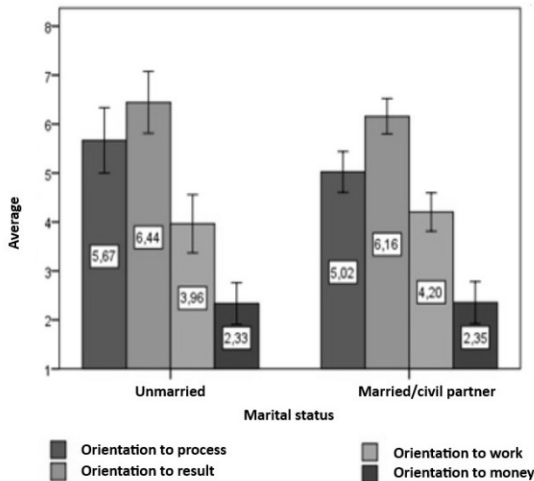


Fig.2. Job orientation (marital status variable)

The results seen in Fig. 2 indicate that the author was wrong in his assumption that marital status is a significant factor in regards to work orientation. There is a slight difference seen in Table II, that differences are not significant.

TABLE II JOB ORIENTATION (MARITAL STATUS VARIABLE) (INDEPENDENT SAMPLES TEST)

	t-test for Equality of Means		
	t	df	Sig. (2-tailed)
Orientation to process	1,533	113	,128
Orientation to result	,770	113	,443
Orientation to work	-,618	113	,538
Orientation to money	-,046	113	,963

The next criterion by which the answers were grouped is education. According to the author, the criterion is very relevant, because perception, motivation, and desires change. What is interesting, Higher Education was among the explored variables in the questionnaire. Education gained in Soviet Union and today is equal to Master's degree.

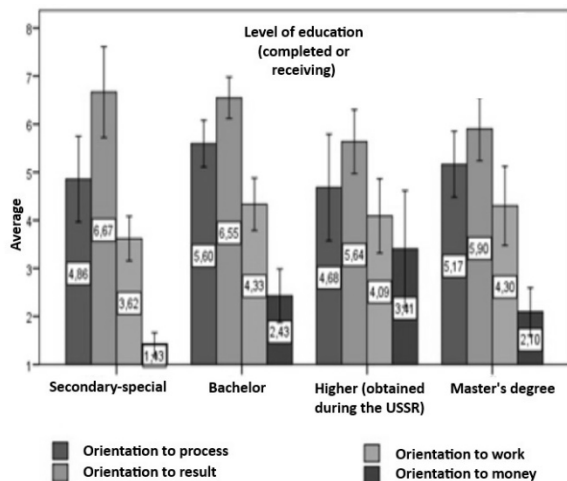


Fig.3. Job orientation ( level of education variable)

Fig. 3 allows to conclude that the structure remains the same: there is a stronger focus on the result rather than on the process; followed by work and money. Employees with a vocational education have been identified as a group, they have the highest orientation towards result, and the lowest for work, practically no orientation to money.

As for the lower education- secondary-special and Bachelor's degree respondents, they have significantly different results in their orientation as compared with the respondents with higher education and Master's degrees.

Employees with higher education are the mostly money-oriented, in comparison with others.

Taking into account all levels of education of all the employees, there are significant differences in the orientation towards money (Table 3).

TABLE III JOB ORIENTATION ACCORDING TO RESPONDENTS LEVEL OF EDUCATION (ANOVA)

	F	Sig.
Orientation to process	1,358	,259
Orientation to result	2,353	,076
Orientation to work	,854	,468
Orientation to money	4,809	,003

Additional income could be considered as an important factor as well, because if the employee is more relaxed, he/she will not have concerns about money, because it is not his/her only source of income, at the same time, the orientation towards money shows why they are employed in several jobs.

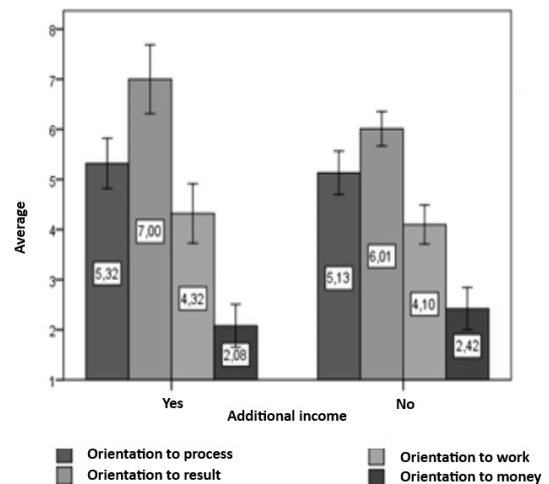


Fig.4. Job orientation breakdown by additional income

In Fig. 4, one sees how the employees layout that is similar to the previous figures: most employees are focused on the result, rather than on the process, work and then followed by money. The orientation to the process and work are practically the same and the orientation to money

higher for those who do not have additional income. Table IV indicates how the orientation towards the result is essential. As well as such large indicator as orientation on the result in no other distribution.

TABLE IV JOB ORIENTATION (ADDITIONAL INCOME VARIABLE) (INDEPENDENT SAMPLES TEST)

	t-test for Equality of Means		
	t	df	Sig. (2-tailed)
Orientation to process	,428	113	,669
Orientation to result	2,671	113	,009
Orientation to work	,547	113	,585
Orientation to money	-,819	113	,414

The level of competence of employees changes its behavior and the way they make decisions, collaborate with colleagues and solve problems in the workplace. It also affects their performance, motivation and attitude to work. Therefore, it was important for the author to include a question about the level of competence.

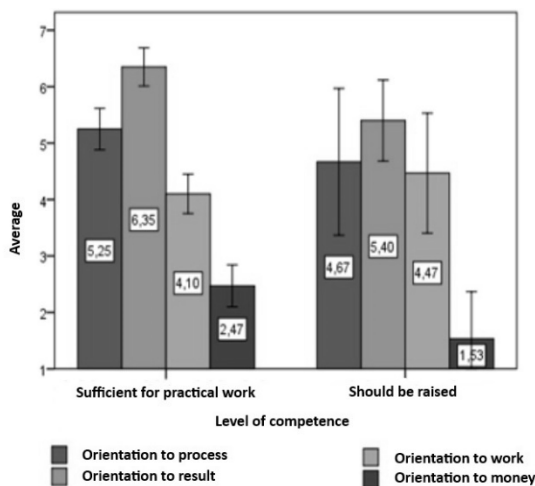


Fig.5. Job orientation breakdown by level of competence

There are very logical results at the level of competence, because those employees who believe that they are not competent enough and need to raise their level of competence – for them the most important thing is work. They tend to work and accumulate experience. They are low creators in other aspects, orientation to money and process, as well as significantly different orientation to the result (Fig. 5). When a person comes to work without experience, he wants to get it and material or other aspects remain on the lowest importance. The opposite situation is with those who believe that the level of competence is sufficient for them, the orientation is less important towards work, but is significantly higher when towards the result and money, and also the orientation towards the process (Table V).

TABLE V JOB ORIENTATION ( LEVEL OF COMPETENCE) (INDEPENDENT SAMPLES TEST)

	t-test for Equality of Means		
	t	df	Sig. (2-tailed)
Orientation to process	1,098	113	,275
Orientation to result	2,070	113	,041
Orientation to work	-,745	113	,458
Orientation to money	1,853	113	,046

The author set the question of the dependents, because it is a responsibility and could affect the employee e.g. by increasing the orientation towards money.

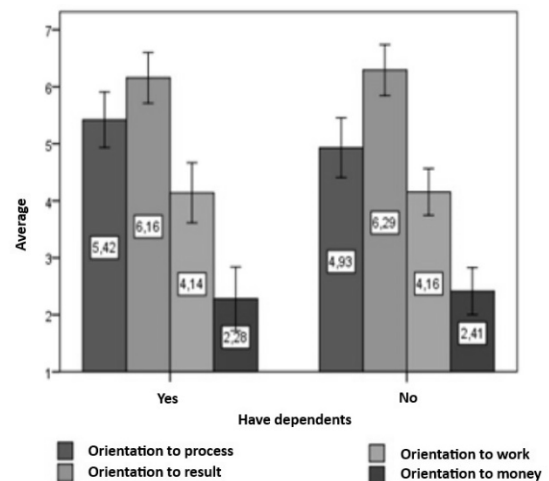


Fig 6. Job orientation

Dependents are not a significant factor, as the indicators are practically the same (Fig. 6). The only difference is the process orientation. However, Table VI allows to conclude that the differences are not significant.

TABLE VI JOB ORIENTATION BREAKDOWN BY HAVE DEPENDENTS (INDEPENDENT SAMPLES TEST)

	t-test for Equality of Means		
	t	df	Sig. (2-tailed)
Orientation to process	1,373	113	,172
Orientation to result	-,430	113	,668
Orientation to work	-,045	113	,964
Orientation to money	-,385	113	,701

Summarizing the obtained results we can conclude that the employee's orientation towards the work process often cannot be influenced by external factors, such as family status or dependent persons. These are more personal characteristics of a person, competences (acquired knowledge and experience) and attitude towards work, which motivate the employee in the current job and determine which priorities are the most important for him at work.

## CONCLUSIONS

The research tool applied for this study is an adopted version of O.Potemkina's questionnaire "Diagnosis of socio-psychological attitudes of a person in the motivational-need sphere" is good tool for exploring the organization of work according to the employee's attitude (currently, a senior customs supervisor needs to know all aspects of work and be able to work in all positions, but in real life there is always not enough time and an employee works more in one position than others), or during the hiring of new employees.

Money-orientation is self-evident, because the work of senior customs officers is a low-paid job, taking into account the negative working environment conditions. Women are more process-oriented, therefore they work more with documents that could be delegated to them, but on the other hand, men are more result-oriented, they are better positioned for roles in combating smuggling from a management perspective. Education is also of great importance, as it drastically changes the difference in results depending on the level of education.

The orientation of senior customs supervisors in the work process often cannot be influenced by external factors, such as marital status or dependents. These are more personal qualities of a person, competencies (acquired knowledge and experience) and attitude to work, which motivate the employee in the current work and determine which priorities are most important for him at work.

This approach could be highly beneficial before a job interview as it would reveal the motivation of the potential employee. If financial considerations are the primary motivation for the applicant, it might indicate that such an employee may not work with the customs for an extended period.

## REFERENCES

- [1] Muitas likums. *Latvijas Vēstnesis*, 119, 2016. Available: <https://likumi.lv/ta/id/283024> [Accessed February 24, 2024].
- [2] Likums "Par Valsts ieņēmumu dienestu". *Latvijas Vēstnesis*, 105, 1993. Available: <https://likumi.lv/ta/id/59902> [Accessed February 24, 2024].
- [3] N.Rudzītis and A. Ceveris, "Development of Customs Fiscal Function in Latvia", *Economics and Business*, vol. 27, no. 1, pp. 23-28, 2015. Available: <https://sciendo.com/article/10.1515/eb-2015-0004> [Accessed February 24, 2024]. <https://doi.org/10.1515/eb-2015-0004>
- [4] О. Потемкина, "Методы диагностики социально-психологических установок личности", Сб. Методы психологической диагностики, Под ред. В.Н. Дружинина, Т.В. Галкиной, вып.1, Москва: ИПРАН, 1993. с. 35-47.
- [5] A.Dodds, A. Farrington, P. Dowler, J. Carruthers, M.Bond, A. L. Jensen and U. Meiser "Get ready for a new mindset on women in customs leadership". *World Customs Journal*, vol. 16, no 1, pp. 117-124, 2022. [Online], Available: [https://worldcustomsjournal.org/Archives/Volume%2016%2C%20Number%201%20\(Mar%202022\)/1930%2002%20WCJ%20v16n1%20Dodds%20et%20al.pdf](https://worldcustomsjournal.org/Archives/Volume%2016%2C%20Number%201%20(Mar%202022)/1930%2002%20WCJ%20v16n1%20Dodds%20et%20al.pdf) [Accessed: February 24, 2024].
- [6] "WCO Annual Report 2020-2021", World Customs Organization, Brussels, Belgium, COMM 2021-1, p. 52, 2021. Available: [https://www.wcoomd.org/-/media/wco/public/global/pdf/about-us/annual-reports/annual-report-2020\\_2021.pdf](https://www.wcoomd.org/-/media/wco/public/global/pdf/about-us/annual-reports/annual-report-2020_2021.pdf) [Accessed February 24, 2024].

# Some Specific Features in the Construction of $p$ -ary Reed-Solomon Codes for an Arbitrary Prime $p$

Zhaneta Savova

Department of Computer Systems and Technologies  
National Military University  
Shumen, Bulgaria  
[zh.savova@yahoo.com](mailto:zh.savova@yahoo.com)

Rosen Bogdanov

Department of Communication Networks and Systems  
National Military University  
Shumen, Bulgaria  
[r61@abv.bg](mailto:r61@abv.bg)

**Abstract.** The Reed-Solomon (RS) codes, proposed in 1960 by Irving Reed and Gustav Solomon as a subset of error-correcting codes, have many current applications. The most significant of which are data recovery in storage systems, including hard drives, minidisks, CDs, DVDs, Google's GFS, BigTable, and RAID 6, as well as in communication systems such as DSL, WiMAX, DVB, ATSC, and satellite communications. Additionally, RS codes are used as Bar codes in management and advertising systems, such as PDF-417, MaxiCode, Datamatrix, QR Code, and Aztec Code. Nowadays, RS codes over Galois Fields  $GF(2^m)$  with base 2 are commonly used in these applications, with the  $GF(2^8)$  field being the most widely used. This allows all 256 values of a byte to be represented as a polynomial with 8 binary coefficients over  $GF(2^8)$ . Considering RS codes as cyclic codes in  $GF(2^m)$  fields, as well as the validity of mathematical dependencies in arbitrary field  $GF(p^m)$ , is a motivation to verify and generalize the idea of generating RS codes in a field with base other prime than 2. As a result, the paper derives the specific features of the construction of Reed-Solomon codes by considering them as a family of codes over any field  $GF(p^m)$  whose base is a prime  $p$  other than 2. The paper also discusses the unique properties of basic arithmetic operations in the arbitrary field  $GF(p^m)$ , which arise from the non-uniqueness of the inverse elements  $a$  and  $-a$  in a field with base other than 2.

**Keywords:** BCH Codes, Error Correcting Codes, Extended Galois Field,  $p$ -ary Reed-Solomon Codes.

## I. INTRODUCTION

The Reed-Solomon (RS) codes are non-binary cyclic error correction codes proposed by Irving Reed and Gustav Solomon in 1960 [1]. By adding symbols to check the data, the RS code can detect any combination of up to a maximum of  $t$  erroneous symbols or correct up to  $\lfloor t/2 \rfloor$

symbols. Here  $\lfloor x \rfloor$  denotes the largest integer less than or equal to  $x$ . Using the RS code as an erasure correction code, it can correct up to a maximum of  $t$  known erasures, or it can detect and correct combinations of errors and erasures. An advantage of RS codes is that they are suitable for correcting burst errors because a sequence of  $m + 1$  bit errors can affect at most two symbols of size  $m$ .

Reed-Solomon codes are most commonly used in data storage systems to correct packet errors caused by media defects. The information recorded on a compact disc (CD) is divided into segments called frames, with each frame containing 24 information symbols. Each symbol is represented as an element of the Galois field  $GF(2^8)$ . The code used to correct errors is called a Cross-Interleaved Reed-Solomon code (CIRC) because it is obtained by a cross-interleaving process of two shortened Reed-Solomon codes [2], [3]. The first code C1, which uses symbols from  $GF(2^8)$  as input information, is the shortened Reed-Solomon code (32, 28). The second code C2 is a shortened (28, 24) Reed-Solomon code again operating in the  $GF(2^8)$ . This sets the rate of the CIRC code to  $r = 24/32 = 3/4 = 0,75$ . Both codes C1 and C2 have a minimum distance  $d_{min} = 5$ , which determines their ability to correct up to a maximum of 2 errors per codeword or to perform up to a maximum of 5 erasure corrections.

Digital Video Discs (DVDs) use a similar error correction scheme called Reed-Solomon Product Code (RS-PC) [4]. In it, the two truncated Reed-Solomon codes C1 and C2 are relatively longer than those in CIRC, being (208, 192) and (182, 172) respectively. In addition, the RS-PC rate is much higher  $r = 172.192/(182.208) = 0.872$ . Blu-ray Discs use an error correction system with an efficient way of indicating packet errors called Picket Code (PC). Pickets are special

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8212>

© 2024 Zhaneta Savova, Rosen Bogdanov. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

columns inserted at regular intervals between the columns of main data. The underlying data is protected by an efficient Reed-Solomon code. The pickets are protected by a second, independent and extremely powerful Reed-Solomon code. During decoding, the pickets are first corrected, and the information obtained can be used to calculate the location of possible errors in decoding the underlying data.

As a result of the use of error correction codes in data storage systems, the maximum packet error length is about 500 bytes for the CIRC code, 2200 bytes for the RS-PC code, while for the PC it is about 9900 bytes. The DVD RS-PC code can reduce the random input error from  $2 \cdot 10^{-2}$  to a data error of  $10^{-15}$ , which is about 10 times better than the CD [4]. Under the same conditions, the possible error in the data on an optical disc using the Pickett code is  $1,5 \cdot 10^{-18}$ , while on an optical disc using RS-PC it is  $5,7 \cdot 10^{-7}$  [5].

Most two-dimensional barcodes, such as QR Code, PDF-417, MaxiCode, Aztec Code, etc., use Reed-Solomon codes to correct errors if part of the barcode is damaged [6]. Modern data transmission systems used in digital television, satellite space and wireless communications use specialized concatenated codes, one of which is the Reed-Solomon code [7], [8].

Erasure-coded storage using Reed-Solomon codes is now widely used in large, distributed storage systems, including Google File System (GFS), Facebook Hadoop Distributed File System (HDFS), Windows Azure storage, and data centers [9], [10], [11].

Nowadays, multi-level signals and sequences are emerging as a prominent feature in today's high-speed communication systems. New methods such as the PWAM signaling scheme [12], 4D PAM-7 [13], and Automotive Ethernet [14] are used in in-vehicle networking. These methods utilize seven-level pulse amplitude modulation (PAM-7), Four-Dimensional Five Level Pulse Amplitude Modulation (4D-PAM-5), and PAM-3 symbols to improve data transfer rates compared to wire infrastructures.

Real-world applications of Reed-Solomon codes mostly use a Galois field representation of  $GF(2^8)$  symbols [15]. In many research papers, the theoretical construction of Reed-Solomon codes is presented over an arbitrary field  $GF(q)$  of  $q$  elements, where  $q$  is a power of a prime number. Despite this theoretical representation, the examples explaining Reed-Solomon codes are over fields of base 2. Therefore, to ensure the error correction features of new multi-level sequences, advanced methods are required to generate not only binary but also nonbinary symbols. The aim of this article is to provide a detailed discussion on constructing Reed-Solomon codes as a family of codes over an arbitrary Galois field  $GF(p^n)$ . It also highlights the unique characteristics of the codes when operating over finite fields of base other prime than 2.

## II. MATERIALS AND METHODS

There are two methods for the construction of Reed-Solomon codes. The first method views the codeword as a sequence of values proposed in Reed and Solomon's

original 1960 paper "Polynomial codes over certain finite fields" [1]. The second method views Reed-Solomon codes as Bose-Chaudhuri-Hocquenghem (BCH) codes [16], where the codeword is represented as a sequence of coefficients.

### A. Original Presentation of Reed-Solomon Codes

Reed and Solomon consider a field  $K$  of degree  $n$  over a field  $Z_2$  of 2 elements [1]. They propose a code  $E$  by which each  $k$ -tuple  $(a_0, a_1, \dots, a_{k-1})$  of  $K$  is matched by a  $2^n$ -tuple  $(m(0), m(\alpha), m(\alpha^2), \dots, m(1))$  of  $K$ . Here  $m(x)$  is a polynomial of degree  $k-1$

$$m(x) = a_0 + a_1x + a_2x^2 + \dots + a_{k-1}x^{k-1}, \quad (1)$$

where  $a_i \in K$ ,  $k < 2^n$ , and  $\alpha$  is the primitive  $n$ -th unit root in  $K$ . Here, the  $k$ -tuple represents the encoded message and the  $2^n$ -tuple represents the transmitted message. The authors prove that this code corrects  $(2^n - k)/2$  or  $(2^n - k - 1)/2$  symbols, depending on whether  $k$  is an even or odd number.

### B. BCH Representation of Reed-Solomon Codes

Instead of sending all values of message polynomial  $m(x)$  (1), the transmitter computes another polynomial  $s(x)$  of degree at most  $n-1$  (where  $n = q-1$ ) and sends the  $n$  coefficients of this polynomial. The polynomial  $s(x)$  is obtained by multiplying the message polynomial  $m(x)$  of degree at most  $k-1$  by the generator polynomial  $g(x)$  of degree  $n-k$ , which is used in the transmitter and receiver of the coding system.

The generating polynomial  $g(x)$  is defined as a polynomial whose roots are the elements  $\alpha, \alpha^2, \dots, \alpha^{n-k}$  of the field  $K$ . Thus,  $g(x)$  can be expressed as:

$$\begin{aligned} g(x) &= (x - \alpha)(x - \alpha^2) \dots (x - \alpha^{n-k}) = \\ &= g_0 + g_1x + \dots \\ &\quad + g_{n-k-1}x^{n-k-1} + x^{n-k}. \end{aligned} \quad (2)$$

The transmitter sends  $n = q - 1$  polynomial coefficients

$$s(x) = m(x)g(x). \quad (3)$$

The receiver considers the received symbols as coefficients of the polynomial  $r(x)$ . If there are no transmission errors ( $r(x) = s(x)$ ), then by dividing the polynomial  $r(x)$  by  $g(x)$  the message polynomial  $m(x)$  can be obtained

$$\frac{r(x)}{g(x)} = m(x). \quad (4)$$

If transmission errors occur, the division will produce a remainder  $e(x)$  with a lower degree than that of  $g(x)$ , indicating the presence of errors, i.e.

$$r(x) = m(x) \cdot g(x) + e(x). \quad (5)$$

If there is an error  $e(x) \neq 0$ , the receiver can calculate  $r(x)$  for all roots of  $g(x)$ . This will result in a system of equations that will determine which coefficients have errors and the values of those errors. The Berlekamp-Messy algorithm [17] or extended Euclidean algorithm [18], and the parity polynomial

$$h(x) = (x - \alpha^0)(x - \alpha^{n-k+1}) \dots (x - \alpha^{n-1}) \quad (6)$$

$$= h_0 + h_1x + \dots + h_{k-1}x^{k-1} + x^k$$

are used to accomplish this.

### C. Key Features of Reed-Solomon Codes

Reed-Solomon codes are linear block cyclic  $(n, k)$  codes of length  $n$  and size  $k$ . The minimum Hamming distance of the RS  $(n, k)$  code is

$$d_{min} = n - k + 1. \quad (7)$$

For an arbitrary systematic  $(n, k)$  code is satisfied

$$d_{min} \leq n - k + 1, \quad (8)$$

since in any  $(n, k)$  code, a non-zero codeword with a weight of at most  $n - k + 1$  can always be created by resetting all but one of the  $k$  information digits.

The code executed with equality at (8) is called Maximum Distance Separable (MDS). As shown in (7), all RS codes are MDS. MDS codes have special properties because they have the maximum possible  $d_{min}$  at their length  $n$  and size  $k$ . For instance, any set of  $k$  columns of their generator matrix  $\mathbf{G}$  are linearly independent, meaning any  $k$  positions in the block can be used as information. Additionally, the weight distribution of MDS codes can be easily determined.

The RS code's correction capabilities are determined by its minimum distance,  $d_{min}$ . It can correct up to  $t = (n - k)/2$  erroneous symbols. If the error locations are known in advance, as defined by the erasure term, the RS code can correct up to a maximum of  $2t$  erasures. The RS code is capable of correcting any combination of errors and erasures, provided that they fall within its correction capabilities

$$2e + s \leq n - k, \quad (9)$$

where  $e$  is the number of errors and  $s$  is the number of erasures in the block.

RS codes cannot be binary since the length  $n$  of the RS code is smaller than the size of the encoding alphabet. RS codes over  $GF(2^m)$  are of particular interest. For instance, for  $m = 8$ , RS codes can have a length of  $n = 2^8 - 1 = 255$  symbols, each 8 bits long.

Since  $GF(2^m)$  is a vector space of size  $m$  over  $GF(2)$ , each element of  $GF(2^m)$  can be represented by  $m$  bits, which are coefficients in the linear combination of selected basis vectors. The element 0 is represented by a zero binary  $m$ -tuple  $(0, 0, \dots, 0)$ , regardless of the chosen basis elements. When using this representation, the  $(n, k)$  code over  $GF(2^m)$  becomes a binary  $(mn, mk)$  code with a minimum distance  $d'_{min}$  at least as large as the minimum distance of the code it forms. This is because each nonzero element of  $GF(2^m)$  has at least one '1' in its binary  $m$ -tuple representation. The case where  $d'_{min} > d_{min}$  is also possible. Therefore, equivalent binary codes are useful for their burst error correction property. Each burst of errors  $(t - 1)m + 1$  or fewer consecutive bits will appear as at most  $t$  errors in the  $GF(2^m)$  symbols. Thus, a decoding algorithm for  $GF(2^m)$  code that corrects all combinations of  $t$  or fewer errors will also automatically correct all bursts of consecutive errors of length less than or equal to  $(t - 1)m + 1$  bits. Reed-Solomon codes are ideal for

correcting burst errors due to their largest possible  $d_{min}$ , given their length  $n = 2^m - 1$  (or a divisor of it) and size  $k$  ( $1 \leq k < n$ ).

Next, we present an algorithm for generating a family of RS codes over an arbitrary field  $GF(p^m)$ , where  $p$  is an arbitrary prime number. For brevity, these codes will be referred to as  $p$ -ary Reed-Solomon codes or pRS codes.

## III. RESULTS AND DISCUSSION

This section provides the mathematical background of an extended Galois field  $GF(p^n)$  and the main steps of the proposed algorithm. It also specifies the algorithm's features for prime  $p$  greater than 2 and give some results from algorithm's testing.

### A. Mathematical Background of an Extended Galois Field $GF(p^n)$

The field  $GF(q)$  is an extension of the Galois Field  $GF(p)$  with a power of  $n$  if the order of  $GF(q)$  can be expressed as a power of the prime  $p$  ( $q = p^n$ ), where  $n$  is a positive ( $n \geq 2$ ). In these cases, we use the notation Extended Galois Field  $GF(p^n)$ .

To create an Extended Galois Field  $GF(p^n)$ , select an irreducible polynomial  $p(x)$  over  $GF(p)$  [19]. Let  $\alpha$  be a root of  $p(x)$  such that  $p(\alpha) = 0$ . The elements of the field  $GF(p^n)$  are polynomials of degree  $n - 1$ , which belong to the ring  $GF(p)[x]$  and have coefficients in  $GF(p)$

$$GF(p^n) = \{a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 \mid a_i \in GF(p)\}. \quad (10)$$

Arithmetic in  $GF(p^n)$  involves polynomial arithmetic modulo the irreducible polynomial  $p(x)$ . The two main algebraic operations are addition (13) and multiplication (14), which are defined for two elements  $f(\alpha)$  (11) and  $g(\alpha)$  (12) of  $GF(p^n)$ .

$$f(\alpha) = \sum_{i=0}^{n-1} a_i \alpha^i = \quad (11)$$

$$= a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0$$

$$g(\alpha) = \sum_{i=0}^{n-1} b_i \alpha^i = \quad (12)$$

$$= b_{n-1}\alpha^{n-1} + \dots + b_1\alpha + b_0$$

Addition in  $GF(p^n)$ :

$$(f(\alpha) + g(\alpha)) = \quad (13)$$

$$= \sum_{i=0}^{n-1} [(a_i + b_i) \bmod p] \cdot \alpha^i \in GF(p^n).$$

Multiplication in  $GF(p^n)$ :

$$r(\alpha) = f(\alpha) \cdot g(\alpha) \bmod p(\alpha) \quad (14)$$

$$= \left( \sum_{k=0}^{2(n-1)} c_k \alpha^k \right) \bmod p(\alpha).$$

The polynomial resulting from the multiplication of  $f(\alpha) \cdot g(\alpha)$  in (14) has coefficients

$$c_k = \sum_{i+j=k} a_i b_j \text{ mod } p, \quad (15)$$

$$0 \leq i \leq n-1, 0 \leq j \leq n-1.$$

An example of the field  $\text{GF}(3^2)$  is used to explain the basic operations in extended Galois fields. The irreducible polynomial  $p(x) = x^2 + x + 2$  is used. Table 1 presents all elements of  $\text{GF}(3^2)$  as polynomials, ordered pairs of coefficients, and powers of the primitive element  $\alpha$ .

TABLE 1 ELEMENTS OF  $\text{GF}(3^2)$  WITH PRIMITIVE POLYNOMIAL  $p(x) = x^2 + x + 2$

№	Representation of $\text{GF}(3^2)$ Elements		
	As a Polynomial	As an Ordered Pair	As a Power of $\alpha$
0	$0 \cdot \alpha + 0$	0 0	0
1	$0 \cdot \alpha + 1$	0 1	$\alpha^0$
2	$0 \cdot \alpha + 2$	0 2	$\alpha^4$
3	$1 \cdot \alpha + 0$	1 0	$\alpha^1$
4	$1 \cdot \alpha + 1$	1 1	$\alpha^7$
5	$1 \cdot \alpha + 2$	1 2	$\alpha^6$
6	$2 \cdot \alpha + 0$	2 0	$\alpha^5$
7	$2 \cdot \alpha + 1$	2 1	$\alpha^2$
8	$2 \cdot \alpha + 2$	2 2	$\alpha^3$

The polynomial and  $n$ -tuple representations are more suitable for addition and subtraction operations, while the power of the primitive element  $\alpha$  representation allows for faster computation of multiplication and division operations. The following formulas will be used:

If  $a = \alpha^x$  and  $b = \alpha^y$  are two elements in  $\text{GF}(p^n)$ , then their product  $c$  is

$$c = a \cdot b = \alpha^x \cdot \alpha^y = \alpha^{(x+y) \text{ mod } (p^n-1)} \quad (16)$$

and their quotient  $d$  is

$$d = \frac{a}{b} = \frac{\alpha^x}{\alpha^y} = \alpha^{(x-y) \text{ mod } (p^n-1)}. \quad (17)$$

As a corollary of equation (17), the multiplicative inverse element  $a^{-1}$  can be determined

$$a^{-1} = \frac{1}{a} = \frac{\alpha^{p^n-1}}{\alpha^x} = \alpha^{(p^n-1-x) \text{ mod } (p^n-1)}. \quad (18)$$

In Example 1 we give the examples of the arithmetic operations addition, subtraction, multiplication, and division of two elements, 2 and 8, from  $\text{GF}(3^2)$ .

**Example 1.** Addition, subtraction, multiplication, and division of elements 2 and 8 from  $\text{GF}(3^2)$ .

**Addition:**  $2 + 8 = 2 + (2 \cdot \alpha + 2) = 2 \cdot \alpha + 1 = 7$ .

**Subtraction:**  $2 - 8 = 2 - 2 \cdot \alpha - 2 = 0 - 2 \cdot \alpha = 1 \cdot \alpha = 3$ .

**Multiplication:**  $2 \cdot 8 = \alpha^4 \cdot \alpha^3 = \alpha^{7 \text{ mod } 8} = \alpha^7 = 4 = 1 \cdot 1$ .

**Division:**  $2/8 = \alpha^4 / \alpha^3 = \alpha^{1 \text{ mod } 8} = \alpha^1 = 3 = 1 \cdot 0$ .

**Multiplicative inverse:**

$2^{-1} = 1/\alpha^4 = \alpha^8/\alpha^4 = \alpha^4 = 2 = 0 \cdot 2$ .

$8^{-1} = 1/\alpha^3 = \alpha^8/\alpha^3 = \alpha^5 = 6 = 2 \cdot 0$ .

As shown in Example 1, in a field with a base other than 2, the inverse additive elements  $a$  and  $-a$  are not unique. Next, we give a specific feature 1, which shows the non-uniqueness of the inverse elements in  $\text{GF}(p)$ ,  $p > 2$ .

**Specific Feature 1.** In Galois Field  $\text{GF}(p)$ , every nonzero element  $a$  has an additive inverse element  $-a = p - a$ .

#### A. Algorithm Main Steps

The pseudocode of the algorithm for generating all  $p$ -ary Reed-Solomon Codes over  $\text{GF}(p^n)$  is shown on Fig. 1.

The first step of the algorithm is to construct a Galois field  $\text{GF}(p)$ . The second step is to construct an extended Galois field  $\text{GF}(p^m)$  by setting  $p(x) = 0$ , where  $p(x)$  is an irreducible polynomial of degree  $m$  in  $\text{GF}(p)$ . Finding the polynomial  $p(x)$  of degree  $m$  is a computationally difficult problem. There are tables of irreducible polynomials for Galois fields of base 2 at various values of  $m$ . For fields with base  $p$  not equal to 2, sophisticated probabilistic algorithms are used to find these polynomials.

Consider the second feature of the algorithm, which involves computing the generator (2) and parity (6) polynomials for  $\text{GF}(p^m)$  with base  $p > 2$ . In some reference works, the subtraction operation in the formulas for computing  $g(x)$  and  $h(x)$  is replaced by addition due to the sameness of the addition and subtraction operations in  $\text{GF}(2^m)$ .

```

algorithm  $p$ -ary Reed-Solomon Codes is
  input: a prime number  $p$ 
           a natural number  $m$ 
  output: all pRS codes in  $\text{GF}(p^m)$  and their
            parameters
  CALL GFp // Construction of a  $\text{GF}(p)$ 
  CALL GFpm // Construction of a  $\text{GF}(p^m)$ 
   $n \leftarrow p^m - 1$ 
  for ( $k = 1$ ;  $k < n$ ;  $k++$ )
  {
    CALCULATE  $g(x)$ ; //Generator polynomial
    CALCULATE  $p(x)$ ; //Parity polynomial
     $d_{\min} \leftarrow n - k + 1$ ; //Hamming distance
     $t \leftarrow \lfloor (n - k)/2 \rfloor$ ; //Number of corrected
    symbols
     $r \leftarrow k/n$ ; //Code Speed
     $b = t/n$ ; //Code Capability
    PRINT  $g(x)$ ,  $p(x)$ ,  $d_{\min}$ ,  $t$ ,  $r$ ,  $b$ ;
  }

```

Fig. 1. Pseudocode of the Algorithm for Generating all pRS Codes over  $\text{GF}(p^n)$ .

**Specific Feature 2.** In formulas (2) and (6), subtraction operations must be performed due to the difference between addition and subtraction operations for fields  $\text{GF}(p^n)$  with base  $p > 2$ .

**Example 2.** Generate a ternary Reed-Solomon code over the Galois field  $\text{GF}(3^2)$  with a length of  $n = 8$  and  $k = 6$  information symbols.

1. Construct the  $\text{GF}(3)$  using the specified arithmetic operations of addition and multiplication:

$$c \equiv a + b \text{ mod } 3$$

$$d \equiv a \cdot b \text{ mod } 3,$$

where  $a, b, c$ , and  $d \in \text{GF}(3)$ .

2. Construct an extended Galois field  $\text{GF}(3^2)$  using the primitive polynomial  $p(x) = x^2 + x + 2$ . To improve the speed of addition and subtraction operations in  $\text{GF}(3^2)$ , elements of the field are represented as ordered pairs. For



multiplication and division operations, elements are represented as powers of the primitive element  $\alpha$  (see Table 1).

3. Generate (8, 6) ternary RS code:

3.1. Calculate the generator polynomial (2):

$$\begin{aligned} g(x) &= (x - \alpha)(x - \alpha^2) = x^2 - \alpha x - \alpha^2 x + \alpha^3 \\ &= x^2 - (\alpha + \alpha^2)x + \alpha^3 \\ &= x^2 - (10 + 21)x + \alpha^3 \\ &= x^2 - 01x + 22 = x^2 + 02x + 22 \end{aligned}$$

3.2. Calculate the parity polynomial (6):

$$\begin{aligned} h(x) &= (x - \alpha^3)(x - \alpha^4)(x - \alpha^5)(x - \alpha^6)(x - \alpha^7)(x - 1) \\ &= (x^2 + \alpha^6 - \alpha^2)(x - \alpha^5)(x - \alpha^6)(x - \alpha^7)(x - 1) \\ &= (x^3 + \alpha^3 x^2 + \alpha^3 x + \alpha^0)(x - \alpha^6)(x - \alpha^7)(x - 1) \\ &= (x^4 + \alpha x^3 + \alpha^6 x^2 + \alpha^2 x + \alpha^2)(x - \alpha^7)(x - 1) \\ &= (x^5 + \alpha^4 x^4 + \alpha^7 x^3 + \alpha^0 x^2 + \alpha^7 x + \alpha^5)(x - 1) \\ &= \alpha^0 x^6 + \alpha^0 x^5 + \alpha^6 x^4 + \alpha^5 x^3 + \alpha^1 x^2 + \alpha^6 x + \alpha^1 \\ &= 01x^6 + 01x^5 + 12x^4 + 20x^3 + 10x^2 + 12x + 10 \end{aligned}$$

4. The code's characteristics are calculated:

- Minimum Hamming distance:  $d_{min} = n - k + 1 = 8 - 6 + 1 = 3$ ;
- Maximum number of error-corrected symbols:  $t = \lfloor (8 - 6)/2 \rfloor = 1$ ;
- Error Correcting Code Speed:  $r = k/n = 100(6/8) = 75\%$ ;
- Error Correcting Code Capability:  $b = t/n = 100(1/8) = 12,5\%$ .

B. Testing the algorithm

The algorithm for generating  $p$ -ary Reed-Solomon codes at arbitrary prime  $p$  is implemented in Visual C#. It is tested for prime values  $p$  between 2 and 13 and all powers  $m$  between 2 and 8. All generated ternary RS codes over the field  $GF(3^2)$  and their parameters are given in Table 2.

Table 3 shows the representation of the elements of the field  $GF(5^2)$  as polynomials, ordered pairs and powers of the primitive element  $\alpha$ . The field  $GF(5^2)$  is constructed using the primitive polynomial  $p(x) = x^2 + x + 2$ . Table 4 shows the 5RS codes over the field  $GF(5^2)$  with even  $n - k$ , which are more widely used because they maximize  $t$  at the corresponding  $k$ .

TABLE 2 3RS CODES OVER  $GF(3^2)$

№	$g(x), h(x)$	$n$	$k$	$d_{min}$	$t$	$r$ [%]	$b$ [%]
1	$g(x) = 10 + 10x + 10x^2 + 10x^3 + 10x^4 + 10x^5 + 10x^6 + 10x^7$ $h(x) = 20 + 10x$	8	1	8	3	12,5	37,5
2	$g(x) = 02 + 20x + 01x^2 + 11x^3 + 12x^4 + 21x^5 + 10x^6$ $h(x) = 11 + 12x + 10x^2$	8	2	7	3	25	37,5
3	$g(x) = 22 + 11x + 12x^2 + 22x^3 + 12x^4 + 10x^5$ $h(x) = 01 + 01x + 21x^2 + 10x^3$	8	3	6	2	25	37,5
4	$g(x) = 12 + 20x + 12x^2 + 11x^3 + 10x^4$ $h(x) = 12 + 20x + 12x^2 + 11x^3 + 10x^4$	8	4	5	2	50	25
5	$g(x) = 12 + 11x + 01x^2 + 10x^3$ $h(x) = 12 + 22x + 22x^2 + 01x^3 +$	8	5	4	1	62,5	12,5

№	$g(x), h(x)$	$n$	$k$	$d_{min}$	$t$	$r$ [%]	$b$ [%]
	$02x^4 + 10x^5$						
6	$g(x) = 22 + 20x + 10x^2$ $h(x) = 01 + 21x + 01x^2 + 02x^3 + 21x^4 + 10x^5 + 10x^6$	8	6	3	1	75	12,5
7	$g(x) = 02 + 10x$ $h(x) = 11 + 21x + 02x^2 + 20x^3 + 22x^4 + 12x^5 + 01x^6 + 10x^7$	8	7	2	0	87,5	0

It should be noted that the coefficients of the computed polynomials  $g(x)$  and  $p(x)$ , shown in Tables 2 and 4, start from the least significant coefficient, i.e. they are written in the reverse order to those in Tables 1 and 3. The reason for this is the generalization of the algorithm to generate pRS codes at different powers  $m$  of the extended field  $GF(p^m)$ . For example, if the  $GF(3^3)$  is used, then the element 5 ( $0.\alpha^2 + 1.\alpha + 2$ ) of the extended Galois field is represented by the 3-tuple 210 as an output of the proposed algorithm.

TABLE 3 ELEMENTS OF  $GF(5^2)$  WITH PRIMITIVE POLYNOMIAL  $P(x) = x^2 + x + 2$

№	As a Polyno mial	As an Ordered Pair	As a Power of $\alpha$	№	As a Polyno mial	As an Ordered Pair	As a Power of $\alpha$
0	$0.\alpha + 0$	0 0	0	13	$2.\alpha + 3$	2 3	$\alpha^{16}$
1	$0.\alpha + 1$	0 1	$\alpha^0$	14	$2.\alpha + 4$	2 4	$\alpha^{20}$
2	$0.\alpha + 2$	0 2	$\alpha^6$	15	$3.\alpha + 0$	3 0	$\alpha^{19}$
3	$0.\alpha + 3$	0 3	$\alpha^{18}$	16	$3.\alpha + 1$	3 1	$\alpha^8$
4	$0.\alpha + 4$	0 4	$\alpha^{12}$	17	$3.\alpha + 2$	3 2	$\alpha^4$
5	$1.\alpha + 0$	1 0	$\alpha^1$	18	$3.\alpha + 3$	3 3	$\alpha^{11}$
6	$1.\alpha + 1$	1 1	$\alpha^{17}$	19	$3.\alpha + 4$	3 4	$\alpha^9$
7	$1.\alpha + 2$	1 2	$\alpha^{14}$	20	$4.\alpha + 0$	4 0	$\alpha^{13}$
8	$1.\alpha + 3$	1 3	$\alpha^{15}$	21	$4.\alpha + 1$	4 1	$\alpha^{22}$
9	$1.\alpha + 4$	1 4	$\alpha^{10}$	22	$4.\alpha + 2$	4 2	$\alpha^3$
10	$2.\alpha + 0$	2 0	$\alpha^7$	23	$4.\alpha + 3$	4 3	$\alpha^2$
11	$2.\alpha + 1$	2 1	$\alpha^{21}$	24	$4.\alpha + 4$	4 4	$\alpha^5$
12	$2.\alpha + 2$	2 2	$\alpha^{23}$				

TABLE 4 5RS CODES OVER  $GF(5^2)$

№	$g(x), h(x)$	$n$	$k$	$d_{min}$	$t$	$r$ [%]	$b$ [%]
1	$g(x) = 04 + 20x + 01x^2 + 33x^3 + 44x^4 + 24x^5 + 22x^6 + 14x^7 + 21x^8 + 30x^9 + 02x^{10} + 12x^{11} + 13x^{12} + 42x^{13} + 11x^{14} + 34x^{15} + 23x^{16} + 43x^{17} + 40x^{18} + 03x^{19} + 41x^{20} + 32x^{21} + 10x^{22}$ $h(x) = 22 + 23x + 10x^2$	24	2	23	11	8,33	45, 83
2	$g(x) = 30 + 32x + 31x^2 + 11x^3 + 44x^4 + 14x^5 + 43x^6 + 23x^7 + 04x^8 + 42x^9 + 41x^{10} + 22x^{11} + 03x^{12} + 04x^{13} + 12x^{14} + 04x^{15} + 22x^{16} + 21x^{17} + 31x^{18} + 03x^{19} + 10x^{20}$ $h(x) = 30 + 23x + 40x^2 + 02x^3 + 10x^4$	24	4	21	10	16, 66	41, 66
3	$g(x) = 24 + 11x + 41x^2 + 02x^3 + 41x^4 + 22x^5 + 24x^6 + 01x^7 + 33x^8 + 11x^9 + 32x^{10} + 33x^{11} + 30x^{12} + 03x^{13} + 33x^{14} + 04x^{15} + 12x^{16} + 43x^{17} + 10x^{18}$ $h(x) = 43 + 33x + 22x^2 + 22x^3 + 23x^4 + 12x^5 + 10x^6$	24	6	19	9	25	37,5
4	$g(x) = 32 + 01x + 43x^2 + 34x^3 + 14x^4 + 21x^5 + 03x^6 + 32x^7 + 33x^8 + 22x^9 + 43x^{10} + 33x^{11} + 34x^{12} + 04x^{13} + 24x^{14} + 34x^{15} + 10x^{16}$ $h(x) = 42 + 11x + 22x^2 + 31x^3 + 10x^4 + 14x^5 + 04x^6 + 21x^7 + 10x^8$	24	8	17	8	33, 33	33, 33
5	$g(x) = 43 + 21x + 31x^2 + 33x^3 + 13x^4$	24	10	15	7	41,	29,

№	$g(x), h(x)$	$n$	$k$	$d_{min}$	$t$	$r$ [%]	$b$ [%]
	$g(x) = 22x^5 + 04x^6 + 32x^7 + 14x^8 + 11x^9 + 33x^{10} + 22x^{11} + 40x^{12} + 42x^{13} + 10x^{14}$ $h(x) = 24 + 42x + 11x^2 + 23x^3 + 02x^4 + 12x^5 + 32x^6 + 14x^7 + 42x^8 + 13x^9 + 10x^{10}$					66	16
6	$g(x) = 20 + 21x + 32x^2 + 33x^3 + 11x^4 + 21x^5 + 31x^6 + 01x^7 + 31x^8 + 42x^9 + 40x^{10} + 12x^{11} + 10x^{12}$ $h(x) = 20 + 34x + 32x^2 + 22x^3 + 11x^4 + 34x^5 + 31x^6 + 04x^7 + 31x^8 + 13x^9 + 40x^{10} + 43x^{11} + 10x^{12}$	24	12	13	6	50	25
7	$g(x) = 02 + 21x + 01x^2 + 34x^3 + 03x^4 + 22x^5 + 13x^6 + 23x^7 + 32x^8 + 30x^9 + 10x^{10}$ $h(x) = 44 + 10x + 31x^2 + 01x^3 + 40x^4 + 11x^5 + 12x^6 + 21x^7 + 41x^8 + 03x^9 + 24x^{10} + 44x^{11} + 13x^{12} + 20x^{13} + 10x^{14}$	24	14	11	5	58, 33	20, 83
8	$g(x) = 40 + 01x + 22x^2 + 02x^3 + 13x^4 + 14x^5 + 44x^6 + 14x^7 + 10x^8$ $h(x) = 10 + 01x + 01x^2 + 41x^3 + 14x^4 + 20x^5 + 24x^6 + 32x^7 + 24x^8 + 02x^9 + 43x^{10} + 24x^{11} + 41x^{12} + 04x^{13} + 03x^{14} + 41x^{15} + 10x^{16}$	24	16	9	4	66, 66	16, 66
9	$g(x) = 12 + 11x + 22x^2 + 11x^3 + 32x^4 + 24x^5 + 10x^6$ $h(x) = 31 + 22x + 41x^2 + 01x^3 + 14x^4 + 44x^5 + 24x^6 + 03x^7 + 22x^8 + 22x^9 + 32x^{10} + 44x^{11} + 20x^{12} + 01x^{13} + 33x^{14} + 02x^{15} + 43x^{16} + 31x^{17} + 10x^{18}$	24	18	7	3	75	12,5
10	$g(x) = 41 + 32x + 42x^2 + 33x^3 + 10x^4 + 41x^5 + 11x^6 + 13x^7 + 04x^8 + 32x^9 + 34x^{10} + 33x^{11} + 24x^{12} + 11x^{13} + 12x^{14} + 43x^{15} + 31x^{16} + 34x^{17} + 22x^{18} + 22x^{19} + 10x^{20}$ $h(x) = 34 + 42x + 31x^2 + 04x^3 + 12x^4 + 41x^5 + 11x^6 + 13x^7 + 04x^8 + 32x^9 + 34x^{10} + 33x^{11} + 24x^{12} + 11x^{13} + 12x^{14} + 43x^{15} + 31x^{16} + 34x^{17} + 22x^{18} + 22x^{19} + 10x^{20}$	24	20	5	2	83, 33	8, 33
11	$g(x) = 24 + 20x + 10x^2$ $h(x) = 43 + 10x + 11x^2 + 01x^3 + 11x^4 + 04x^5 + 02x^6 + 23x^7 + 30x^8 + 42x^9 + 02x^{10} + 03x^{11} + 23x^{12} + 21x^{13} + 43x^{14} + 32x^{15} + 32x^{16} + 03x^{17} + 42x^{18} + 01x^{19} + 21x^{20} + 30x^{21} + 10x^{22}$	24	22	3	1	91, 66	4,16

### CONCLUSIONS

The article proposes an algorithm for generating  $p$ -ary Reed-Solomon codes and identifies two specific features of an algorithm for an arbitrary prime  $p$ , greater than 2.

In the developed algorithm for generating  $p$ -ary Reed-Solomon codes, the most tedious problem is that of constructing an extension of a Galois field  $GF(p^m)$  at an arbitrary prime  $p$ . As  $p$  and  $m$  grow, the time to find a primitive polynomial  $p(x)$  with which to generate the extended field grows exponentially. This also increases the memory required to store the powers of the primitive element  $\alpha$ .

When selecting a suitable RS code, the theoretical and applied aspects of its characteristics must be considered. From a theoretical point of view, the codes are compared in terms of their ability to maximize the channel capacity, which automatically leads to a requirement for a high RS code rate, the signal-to-noise ratio and the number of errors that the code can correct and detect. From an application point of view, the complexity of the implementation, the processing delay, and the evaluation of the possibility of retransmitting the data packet if the errors cannot be corrected are considered. In this respect, the use of a prime number  $p$  greater than two leads to a

reduction in the length of the RS code used to transmit the same amount of information while maintaining the code's ability to correct.

To summarise, the proposed algorithm has a higher time and memory complexity in its first two steps, which are only executed once, compared to the original RS algorithm that operates at base 2. The algorithm's main advantage is that, by using a prime  $p$  greater than 2, it significantly reduces the length of the pRS code while maintaining the same error-correcting capability as the RS code with base 2.

As future work, a speed comparison could be conducted on concrete computational systems between the proposed algorithm running on an arbitrary prime  $p$  and the original algorithm running with prime 2.

### ACKNOWLEDGMENTS:

The article was prepared with the financial support of the National Scientific Program "Security and Defence", funded by the Ministry of Education and Science of the Republic of Bulgaria, in implementation of Decision № 731 of 21.10.2021 of the Council of Ministers of the Republic of Bulgaria.

The authors would like to thank the reviewers for their helpful comments.

### REFERENCES

- [1] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," Journal of the Society for Industrial & Applied Mathematics 8, No. 2, pp. 300-304, 1960.
- [2] H. Hovee, J. Timmermans and L. Vries, "3.4 Error Correction and Concealment in Compact Disc Systems," in Origins and Successors of the Compact Disc, Contributions of Philips to Optical Storage: Springer Link, 2009, pp. 82.
- [3] J. D. Key, "Some error-correcting codes and their applications," in Applied Mathematical Modeling: A Multidisciplinary Approach, Chapman & Hall/CRC Press, 1999.
- [4] H. Chang, C. Shung and C. Lee, "A Reed-Solomon Product-Code (RS-PC) Decoder Chip for DVD Applications," IEEE Journal of Solid-State Circuits, Vol. 36, No. 2, pp. 229-238, February 2001.
- [5] X. Liu, H. Jia and C. Ma, "Error-Correction codes For Optical Disc Storage," in Advances in Optical Data Storage Technology, Proceedings of SPIE Vol. 5643, pp. 342-347, 2005.
- [6] J. A. Lin and C. S. Fuh, "2D Barcode Image Decoding," in Mathematical Problems in Engineering, Article ID 848276, 10 pages, 2013. <https://doi.org/10.1155/2013/848276>.
- [7] A. J. McAuley, "Reliable broadband communication using a burst erasure correcting code," in Proceedings of the ACM symposium on Communications architectures & protocols, pp. 297-306, ACM, 1990, <https://dl.acm.org/doi/pdf/10.1145/99508.99566>.
- [8] H. -C. Lee, J. -H. Wu, C. -H. Wang and Y. -L. Ueng, "A Graph-Based Soft-Decision Decoding Scheme for Reed-Solomon Codes," in IEEE Journal on Selected Areas in Information Theory, vol. 4, pp. 420-433, 2023, <https://doi.org/10.1109/JSAIT.2023.3315453>.
- [9] Y. Chen, "Thermal Management and Data Archiving in Data Centers," Ph.D. thesis, Auburn University, Auburn, Alabama, 2016.
- [10] T. N. Hewage, M. N. Halgamuge, A. Syed, and G. Ekici, "Big data techniques of Google, Amazon, Facebook and Twitter," in Journal of Communications Vol. 13, No. 2, pp. 94-100, February 2018.
- [11] A. Chiniyah and A. Mungur, "On the Adoption of Erasure Code for Cloud Storage by Major Distributed Storage Systems," in EAI Endorsed Transactions on Cloud Systems, 7(21), e1-e11, 2022.
- [12] H.-U. Kim and J.-K. Kang, "High-speed Serial Interface using PWAM Signaling Scheme," in 19th International SoC Design

- Conference (ISOCC), Gangneungsi, Korea, pp. 255-256, 2022, <https://doi.org/10.1109/ISOCC56007.2022.10031330>.
- [13] N. Stojanović, C. Prodaniuc, Z. Liang, J. Wei, S. Calabró, T. Rahman and C. Xie, "4D PAM-7 Trellis Coded Modulation for Data Centers," in IEEE Photonics Technology Letters, Vol. 31, No. 5, pp. 369-372, 1 March 2019, <https://doi.org/10.1109/LPT.2019.2895686>.
- [14] K. Matheus and T. Königseder, Automotive Ethernet. Cambridge University Press, 2021.
- [15] S. Nabipour and M. Gholizade, Arithmetic Operators over Finite Field GF ( $2^m$ ) in BCH and Reed-Solomon Codes, arXiv preprint arXiv:2310.12319, 2023, [Online]. Available: <https://arxiv.org/ftp/arxiv/papers/2310/2310.12319.pdf>. [Accessed: Jan. 7, 2024].
- [16] R. C. Bose and D.K. Ray-Chaudhuri. "On a class of error correcting binary group codes," in Information and Control, Volume 3, Issue 1, pp. 68–79, March 1960.
- [17] N. Atti, G. Diaz–Toca and H. Lombardi, The Berlekamp-Massey Algorithm revisited, in Applicable Algebra in Engineering, Communication and Computing 17(1), pp. 75–82, 2006, <https://doi.org/10.1007/s00200-005-0190-z>.
- [18] J. A. M. Naranjo, J. A. López-Ramos and L. G. Casado, "Applications of the extended Euclidean algorithm to privacy and secure communications," in Proceedings of the 10th International Conference on Computational and Mathematical Methods in Science and Engineering, CMMSE 2010, pp. 27–30, June 2010.
- [19] A. Beletsky, "An Effective Algorithm for the Synthesis of Irreducible Polynomials over a Galois Fields of Arbitrary Characteristics," in WSEAS Transactions on Mathematics 20, pp. 508-519, 2021.

# Applicability of JARUS SORA to state UAS operations in disaster relief

**Hristo Stanev**

Faculty "Economics of Infrastructure"  
University of National and World Economy  
Sofia, Bulgaria  
hstanev@e-dnrs.org

**Stefan Hristozov**

Sensors and Measurement Technologies in Robotics &  
Mechatronics Dept.  
Institute of Robotics  
Sofia, Bulgaria  
st.hristozov@ir.bas.bg

**Abstract.** *The use of modern unmanned aviation technologies when conducting search and rescue operations, respectively when overcoming the consequences of disasters is an economically justified approach to increase the effectiveness of operations, reducing the costs of their implementation. The nature of the operations implies working in an environment of high uncertainty with variety of stakeholders, which requires the implementation of additional measures to achieve the target levels of aviation safety. To tackle the risks associated with any Unmanned Aerial Systems (UAS) operations JARUS (Joint Authorities for Rulemaking in Unmanned Systems) has proposed a document called SORA (Specific Operations Risk Assessment) adopted as acceptable means of compliance by many civil aviation authorities.*

*Admittedly, SORA was developed with civil use of UAS in mind. However, considering its comprehensiveness in risk assessment it is a good starting point to evaluate its applicability at disaster relief operations and adaptability to state aircraft operations. As a rule, activities to overcome the consequences of disasters are the responsibility of the state, therefore it is normal to expect that the capabilities to use UAS will be created and predetermines the relevance of the presented topic.*

*In the current article the team analyses SORA applicability from the perspective of emergency services as state aircraft operations. Thus, the purpose of this article is to explore the possibilities and to justify the need of implementing a timely procedure and to show an example risk analysis performed for this type of operations, when operating with state unmanned aircraft. Of course, some of the conclusions drawn here for emergency services can be easily transposed to other state UAS operations.*

**Keywords:** *JARUS SORA, state UAS, applicability, disaster relief.*

## I. INTRODUCTION

The use of Unmanned Aerial Systems (UAS) to conduct operations in the event of disasters, accidents and catastrophes has established itself as a standard approach to reduce the costs of their conduct, as well as to increase the speed of response while ensuring high levels of aviation safety. There are already many studies in the literature on

their application in this field – aerial surveillance for forest fires [1] and firefighting [2], search and rescue missions [3], [4], prevention of disasters [5] and disaster management [6], [7]. Almost all reviews do not take into account the fact that UAS can be used in either their civilian or state capacity. In most cases, civil regulations for UA flights are assumed to be followed, which explains the lack of publications regarding the applicability of JARUS SORA in state UAS operations [8].

On the other hand, it is observed that the International Civil Aviation Organization (ICAO) policy of non-interference in the internal affairs of member states continues to be implemented, not developing the problems of state aviation in ICAO documents, as they are of own responsibility. In the Convention on International Civil Aviation [8], the general understanding of state aircraft is adopted, without speaking of state aviation. In fact, the combination of state aircraft, specialized infrastructure (airports, communication and navigation equipment) and rules for their use predetermines the presence of state aviation in the country where they were created.

An important clarification to introduce into the issues on the subject is the correct understanding of the concept of state aircraft (SA). In Art. 3 of the ICAO, it is accepted that the convention applies to civil aircraft (CA) and does not apply to SA. Those aircraft used in military, customs and police services are considered as SA. From here comes the understanding that the registration of the aircraft is irrelevant - whether it is in a registry of civil aircraft or in a registry of military aircraft (MA), it is only important that they work in the interest of one of the three state services. The same approach should be applied to UAS. Therefore, there may be cases where military, customs or police special operations use civil aircraft flying according to operational flight rules."

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8195>

© 2024 Hristo Stanev, Stefan Hristozov. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

Here JARUS has the vision to provide timely consensus recommendations for UAS that meet the common needs of JARUS members and stakeholders, including ICAO [9] and comes with a document called SORA – Specific Operations Risk Assessment, developed by Working Group 6 Safety and Risk Management, which now has its 2.0 version (by the time the article is prepared 2.5 is under public consultation). The SORA is meant to help operators and competent authorities and highlight the benefits of a harmonized risk assessment methodology. [10]

## II. ANALYSIS OF SORA METHODOLOGY

The SORA Methodology 2.0 [10] in Fig. 1 comprises of ten systematic steps, each crucial for evaluating the safety aspects of Unmanned Aircraft Systems (UAS) operations. Herein, we delineate each step along with its significance within the framework:

1. **Documentation of Proposed Operations:** This initial step serves as a foundational tool for communication between the applicant and the Competent Authority. It involves the creation of comprehensive documentation encompassing operator manuals, compliance evidence, and risk assessments. These documents elucidate the nature of the UAS operation, including flight path details, airspace type, and population density overflow.

2. **Intrinsic Ground Risk Class (iGRC):** The determination of iGRC, scaled from 1 to 11, is pivotal and hinges upon UA characteristics and population density. This assessment is conducted for both the area at risk and its adjacent region.

3. **Final Ground Risk Class:** Considering strategic mitigations, this step calculates the Final Ground Risk Class, crucial for evaluating the potential fatality risks associated with the operation.

4. **Initial Air Risk Class (ARC):** Assessment of ARC, conducted qualitatively, involves evaluating airspace characteristics identified in Step #1. Parameters defining ARC categories include airspace type, altitude, and urbanization levels.

5. **Residual Air Risk Class:** Following strategic mitigations, this step determines the Residual Air Risk Class, aiming to reduce the initial risk level associated with mid-air collisions.

6. **Tactical Mitigation Performance Requirement (TMPR) and Robustness Levels:** Tactical mitigations are implemented during operations to mitigate residual risks. TMPRs address various functional aspects crucial for risk mitigation.

7. **Specific Assurance and Integrity Level (SAIL) Determination:** Utilizing outputs from previous steps, SAIL is determined to gauge the operational integrity and assurance level required for the UAS operation.

8. **Identification of Containment Requirements:** This step focuses on assessing risks posed by operational loss of control, necessitating containment design features and operational procedures to mitigate potential hazards.

9. **Identification of Operational Safety Objectives (OSO):** Based on the assigned SAIL, OSOs are identified, specifying integrity and assurance levels required for

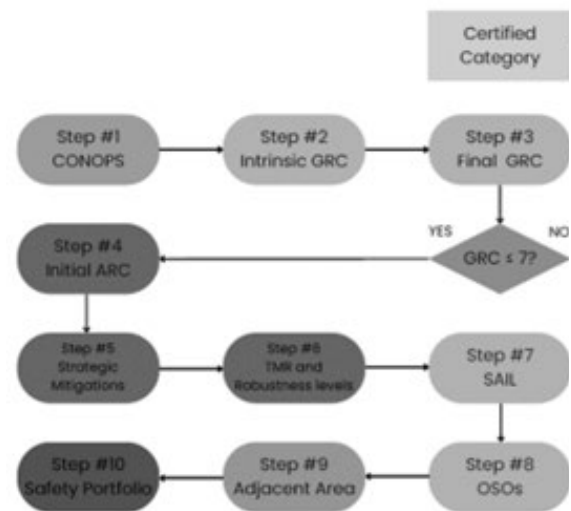


Fig. 1 SORA Methodology (source UAV Navigation-Grupo Oesía)

various operational aspects, including UAS technical functionalities and human factors.

10. **Comprehensive Safety Portfolio:** This final step involves compiling a comprehensive safety portfolio comprising all necessary documents and compliance evidence, ensuring alignment with SORA requirements. Any discrepancies may necessitate adjustments to the proposed operation or additional evidence for compliance.

By adhering to these systematic steps, the SORA methodology facilitates a rigorous assessment of UAS operations, ensuring safety and regulatory compliance.

Regarding the operations with state UAS, when participating in the disaster relief operations, the applicability of the entire SORA methodology should be assessed in view of the need for a rapid response in the absence of basic information about the area of operations [11], [12]. The assumptions are that SORA can only be applied if there are risk mitigation measures in place beforehand. Regarding the ground risk assessment, there is no doubt that it should be complete in both cases (use of UAS as civil or state), but the risk reduction measures allow to minimize the air risk to allow operations to take place with state UAS in disasters by uncertified personnel according to the requirements of civil aviation. The purpose of the proposed preliminary steps is to minimize the air risk to reasonable limits.

## III. EXAMPLE SCENARIO

As of 2011, wildfires around Bansko and Simitli, located in Bulgaria, were a significant concern due to their potential impact on the environment, economy, and public safety. Bansko is a popular ski resort town situated in the Pirin Mountains, while Simitli is a municipality located in the Blagoevgrad Province, also in the southwestern part of Bulgaria.

Wildfires such regions, particularly during dry and hot periods, pose a threat to the surrounding forests, biodiversity, and nearby communities. The Pirin Mountains, where Bansko is located, are known for their diverse ecosystems, including old-growth forests

and unique plant species. Fires in these areas can lead to habitat destruction, soil erosion, and loss of biodiversity.

Simitli, being situated in a region with a mix of forests and agricultural lands, is also susceptible to wildfires. In addition to the ecological impact, wildfires in this area can pose risks to agricultural crops, livestock, and rural communities.

UAS can play a crucial role in various aspects of wildfire management and prevention efforts in regions like Bansko and Simitli. Utilizing UAS for forest fire monitoring offers several advantages, including enhanced situational awareness, rapid response capabilities, and reduced risk to human personnel. During wildfire incidents, UAS equipped with infrared cameras and smoke-penetrating sensors can provide real-time data on fire behaviour, smoke dispersion, and hotspots to incident commanders and firefighting crews. This information can help optimize resource allocation, tactical decision-making, and deployment of ground and aerial firefighting assets. UAS can also serve as aerial scouts, providing reconnaissance of fire lines, access routes, and safety zones for firefighting personnel.

#### IV. SORA PREPARATIONS & APPLICATION

Considering the Example Scenario as a basis for the ConOps, a progress can be made towards SORA 2.0 methodology.

##### Step #1

For Step #1 of SORA, ConOps description, we consider the following UA and type of mission for the current operation:



Fig. 2 Area of Operations

- Size of UA 2.5m
- Speed of UA 30 m/s
- ~ K.E. of UA 6750J
- Max Pop Density 660 ppl/km<sup>2</sup>
- VLOS/BVLOS? BVLOS
- Altitude 4000 feet AGL
- Adjacent Area Not considered
- Average Pop Density 42 ppl/km<sup>2</sup>

The area of operation is located on the West of the town of Bansko, in the Pirin National Park, with coordinates 41.8368562615972, 23.422988726663785 – Fig. 2

##### Step #2 & #3

SORA requires pretty straightforward determination of iGRC. Step #3 defines means to mitigate it.

The area of the example scenario is located West of the town of Bansko with the following characteristics of population (Fig. 3):

- Density 12,348 ppl/km<sup>2</sup>
- Count 660 People

TABLE 1 is taken directly from SORA 2.0 and depicts the iGRC utilized in determining the GRC. It shows the GRC determined based on the operational scenario and the maximum characteristic dimension of the UA, which determines the lethal area of the UAS. If there is a discrepancy between the maximum UA characteristic dimension and the anticipated kinetic energy, the applicant must justify the selected column.

TABLE 1 INTRINSIC UAS GROUND RISK CLASS DETERMINATION TABLE

Max UAS characteristics dimension	1 m / approx. 3ft	3 m / approx. 10ft	8 m / approx. 25ft
Typical kinetic energy expected	< 700 J (approx. 529 Ft Lb)	< 34 KJ (approx. 25000 Ft Lb)	< 1084 KJ (approx. 80000 Ft Lb)
<b>Operational scenarios</b>			
VLOS/BVLOS over controlled ground area	1	2	3
VLOS in sparsely populated environment	2	3	4
BVLOS in sparsely populated environment	3	4	5
VLOS in populated environment	4	5	6
BVLOS in populated environment	5	6	8

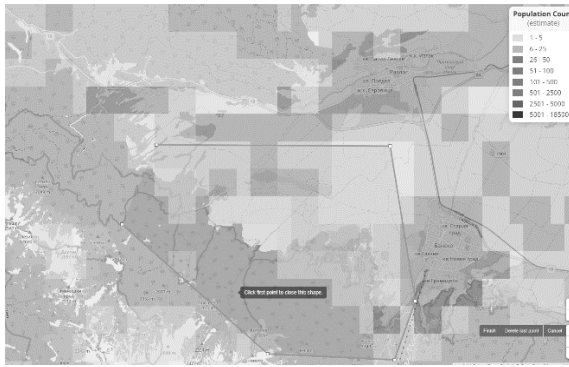


Fig. 3 Population Density Heat Map

The Final GRC determination (Step #3) is based on the availability of these mitigations to the operation. TABLE 2 provides a list of potential mitigations and the associated relative correction factor. A positive number denotes an increase of the GRC, while a negative number results in a decrease of the GRC.

The claims available in Annex B of SORA, that are made, are:

**For M1:**

- Integrity – the applicant evaluates the area of operations by means of on-site inspections/appraisals to justify lowering the density of people at risk (e.g. residential area during daytime when some people may not be present or an industrial area at night time for the same reason).
- Assurance – the applicant declares that the

TABLE 2 LIST OF POTENTIAL MITIGATION FACTORS (ANNEX B)

Mitigation Sequence	Mitigations for ground risk	Robustness		
		Low/None	Medium	High
1	M1 – Strategic mitigations for ground risk	0: None -1: Low	-2	-4
2	M2 – Effects of ground impact are reduced	0	-1	-2
3	M3 – An Emergency Response Plan (ERP) is in place, operator validated and effective	1	0	-1

required level of integrity has been achieved

**For M2:**

- Integrity – Any equipment used to reduce the effect of the UA impact dynamics are installed and maintained in accordance with manufacturer instructions
- Assurance – 1. Procedures are validated against standards considered adequate by the competent authority and/or in accordance with means of compliance acceptable to that authority.  
2. The adequacy of the procedures is proved through:
  - Dedicated flight tests, or
  - Simulation, provided that the representativeness of the simulation means is proven for the intended purpose with positive results.

**For M3:**

- Integrity – the ERP:
  - is suitable for the situation;
  - limits the escalating effects;
  - defines criteria to identify an emergency situation;
  - is practical to use;
  - clearly delineates Remote Crew member(s) duties.
- Assurance – 1. An ERP training syllabus is available.  
2. A record of the ERP training completed by the relevant staff is established and kept up to date

**Determination of Initial Air Risk Class (iARC) (Step #4 & #5):**

The ARC is a qualitative categorization representing the likelihood of a UAS encountering a

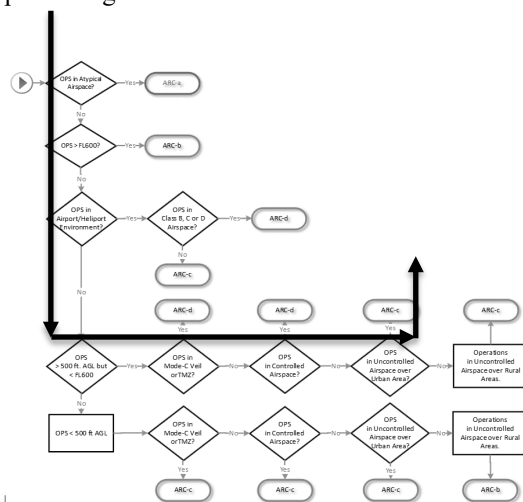


Fig. 4 ARC assignment process from JARUS guidelines on Specific Operations Risk Assessment (SORA)

manned aircraft within typical generalized civil airspace. It serves as an initial assessment of the

combined collision risk for the airspace, before any mitigating measures are implemented.

In view of the fact that in order to achieve higher efficiency of unmanned aircraft UA flights over natural disaster areas, flights are required to be conducted at altitudes above 500 ft, it is no longer necessary to comply with the requirements for flights up to 500 ft. Take-off and landing are always carried out in visual line of sight (VLOS), which is within this altitude, and an ad-hoc danger zone may not be designated as long as the responsibility for avoiding collision with other aircraft rests with the UAS operator and he is able to provide it.

As previously mentioned, ARC serves as a generalized qualitative assessment of the likelihood of a UAS encountering a manned aircraft within a specific airspace environment. However, it's acknowledged that the collision risk within the UAS Operational Volume may differ from the initially assigned ARC.

Strategic mitigations are implemented by controlling the airspace infrastructure through physical characteristics, procedures, and techniques aimed at reducing conflicts or facilitating conflict resolution.

Looking ahead, as Unmanned Traffic Management (UTM) and U-Space become more defined and widely adopted, they will offer a framework for UAS operators to apply strategic mitigations based on common procedures and rules in the airspace. This will enable more effective management of collision risk in UAS operations.

For the current scenario if the Flowchart from SORA 2.0 is used the iARC ends up in ARC-c. This might not be true for state operator with predefined procedures to deploy an ad-hoc danger zone and convert the area of operations into Atypical Airspace.

**Step #6: Tactical Mitigation Performance Requirement (TMPR)**

Operation Requirements:

Modifications to the initial and subsequent approvals may be necessary as safety and operational issues arise, as determined by the competent authority or Air Navigation Service Provider (ANSP).

It is essential for both the operator and competent authority to recognize that the Air Risk Classes (ARCs) provide a generalized qualitative classification of collision risk. Local circumstances, such as special events, may invalidate the assumptions regarding aircraft density made in the SORA.

Therefore, it is imperative for both parties to have a comprehensive understanding of the local airspace and air traffic flows. Developing a system that can promptly alert operators to changes in the airspace on a local level is crucial. This will enable operators to effectively address the increased risks associated with such events and ensure safe operations. Such discussion is outside of the current research.

**Step #7: Specific Assurance and Integrity Level (SAIL) Determination**

The SAIL parameter integrates ground and air risk analyses, guiding necessary actions to be taken. It signifies

the level of confidence in the UAS operation's ability to remain under control.

Following the determination of the Final GRC and Residual ARC, the SAIL associated with the proposed ConOps can be derived.

The SAIL is qualitative and reflects:

- Operational Safety Objectives (OSO) to be adhered to,
- Description of activities facilitating compliance with these objectives, and
- Evidence demonstrating the fulfilment of these objectives.

The assignment of SAIL to a specific ConOps is determined using TABLE 3.

TABLE 3 SAIL DETERMINATION

Final GRC	Residual ARC			
	a	b	c	d
≤2	I	II	IV	VI
3	II	II	IV	VI
4	III	III	IV	VI
5	IV	IV	IV	VI
6	V	V	V	VI
7	VI	VI	VI	VI
>7	Certified operation			

**Step #8: Identification of Operational Safety Objectives (OSO)**

In the final step of the SORA process, the Specific Assurance and Integrity Level (SAIL) is utilized to assess the defenses within the operation by defining Operational Safety Objectives (OSO) and determining their corresponding level of robustness.

TABLE 4 below is an extract of Table 6 from SORA 2.0 and offers a qualitative methodology for making this determination. In the table, the designation "O" indicates an optional objective, "L" denotes a recommendation with low robustness, "M" suggests a recommendation with medium robustness, and "H" signifies a recommendation with high robustness.

The OSOs are categorized based on the threats they help mitigate, which may result in some objectives being repeated in the table.

**Step #9 – Adjacent Area/Airspace Considerations**

In the specific case, the depicted airspace is located in a Class G airspace and to ensure the safety of other airspace users who are not involved in a disaster operation, it should be done through the definition of ad-hoc danger zones. The zone thus defined can be estimated to be from some lower limit to some upper limit, depending on the opto-electronic equipment used on board the UAS, with safety buffers included in the horizontal and vertical planes. Appropriate safety buffers are 500 ft in the vertical plane and up to 1 NM in the horizontal plane (unless in an urban environment where smaller values may apply depending on terrain and urban infrastructure acting as a natural separation



TABLE 4 OPERATIONAL SAFETY OBJECTIVES

OSO Number (in line with Annex E)		SAIL					
		I	II	III	IV	V	VI
	Technical issue with the UAS						
OSO#01	Ensure the operator is competent and/or proven	O	L	M	H	H	H
OSO#02	UAS manufactured by competent and/or proven entity	O	O	L	M	H	H
OSO#05	UAS is designed considering system safety and reliability	O	O	L	M	H	H
	Human Error						
OSO#18	Automatic protection of the flight envelope from Human Error	O	O	L	M	H	H
	Adverse operating conditions						
OSO#24	UAS designed and qualified for adverse environmental conditions	O	O	M	H	H	H

boundary of operations between manned and unmanned aircraft Take-off and landing in all cases are carried out in conditions of direct visibility, therefore there is no need to define an ad-hoc danger zone.

The SORA process equips the applicant, competent authority, ANSP and the Operator with a comprehensive methodology aimed at ensuring the safe conduct of UAS operations. This methodology includes a series of mitigations and safety objectives to be considered, which are as follows:

- Mitigations utilized to adjust the intrinsic Ground Risk Class (GRC).
- Strategic mitigations addressing the Initial Air Risk Class (ARC).
- Tactical mitigations addressing the Residual Air Risk Class (ARC).
- Considerations for the Adjacent Area/Airspace.
- Operational Safety Objectives.

The satisfactory substantiation of these mitigations and objectives, as required by the SORA process, provides a sufficient level of confidence that the proposed operation can be conducted safely.

## V. DISCUSSIONS

With the application of preliminary measures to reduce aerial risk according to the specific unmanned platforms used in disasters, the possibility of a quick response by drone operators is also achieved. Shortening the time for the preparation of the assessment (write here which final assessment is important from TABLE 4 and what are the differences before and after the application of preliminary measures) also allows increasing the efficiency of operations with unmanned aircraft, while maintaining high levels of aviation safety. A common understanding of prioritizing search and rescue operations over other operations is of utmost importance for timely provision of safe working conditions in the disaster area. Informational

awareness of other airspace users, whether manned or unmanned, is the other key factor without which aviation safety cannot be guaranteed when conducting drone operations in the disaster area.

## CONCLUSION

Overall, effective wildfire management (e.g. Bansko and Simitli) requires a comprehensive and integrated approach that addresses both the immediate response needs and the underlying factors contributing to wildfire risk in the region. Collaboration between government agencies, local communities, and stakeholders is essential for reducing the threat of wildfires and safeguarding the region's natural and cultural resources. Integrating UAS into wildfire management efforts can enhance operational efficiency, improve situational awareness, and contribute to more effective wildfire prevention, detection, and response strategies. However, it's essential to ensure compliance with aviation regulations, privacy considerations, and coordination with existing wildfire management protocols when deploying UAS in fire-prone environments.

The capabilities created by the states to use UAS (state or civil aircraft) in conducting operations in the event of disasters, accidents and catastrophes should be supported in the possibility of being used in short terms. As seen from the results of applying SORA 2.0 to the full scenario and pre-created scenarios, it is quite possible to apply JARUS SORA 2.0 to state UAS disaster relief operations.

It should be noted that in view of the change of the applicable SORA from version 2.0 to version 2.5, this analysis should also be performed according to the requirements of the new methodology. After the adoption of SORA 2.5, it will be possible to analyse the benefits of applying the new methodology compared to

the old one, but with regard to the use of state UAS in operations related to crisis management.

#### ACKNOWLEDGMENTS

This work was supported by the National Scientific Programme “Defence & Security”, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria in execution of Ministry Council Decision No. 731/21.10.2021 under the grant agreement No. D01-74/19.05.2022.

#### REFERENCES

- [1] S. Sudhakar, V. Vijayakumar, C. S. Kumar, V. Priya, L. Ravi and V. Subramaniaswamy, “Unmanned Aerial Vehicle (UAV) based Forest Fire Detection and monitoring for reducing false alarms in forest-fires,” *Computer Communications*, vol. 149, pp. 1-16, 2020.
- [2] B. Aydin, E. Selvi, J. Tao and M. J. Starek, “Use of Fire-Extinguishing Balls for a Conceptual System of Drone-Assisted Wildfire Fighting,” *Drones*, vol. 3, no. 1, p. 17, 2019.
- [3] P. T. Thavasi and C. D. Suriyakala, “Sensors and Tracking Methods Used in Wireless Sensor Network Based Unmanned Search and Rescue System -A Review,” *Procedia Engineering*, vol. 38, pp. 1935-1945, 2012.
- [4] C. V. Tilburg, “First Report of Using Portable Unmanned Aircraft Systems (Drones) for Search and Rescue,” *Wilderness & Environmental Medicine*, vol. 28, no. 2, pp. 116-118, 2017.
- [5] P. Petrides, P. Kolios, C. Kyrkou, T. Theocharides and C. Panayiotou, Disaster Prevention and Emergency Response Using Unmanned Aerial Systems, A. Stratigea, E. Kyriakides and C. Nicolaidis, Eds., Springer International Publishing, 2017, pp. 379-403.
- [6] L. Apvrille, T. Tanzi and J.-L. Dugelay, “Autonomous Drones for Assisting Rescue Services within the Context of Natural Disasters,” in *2014 XXXIth URSI General Assembly and Scientific Symposium (URSI GASS)*, Beijing, China, 2014.
- [7] M. Quaritsch, K. Kruggl, D. Wischounig-Strucl, S. Bhattacharya, M. Shah and B. Rinner, “Networked UAVs as Aerial Sensor Network for Disaster Management Applications,” *e & i Elektrotechnik und Informationstechnik*, vol. 127, no. 3, pp. 56-63, 2010.
- [8] P. Janik, M. Zawistowski, R. Fellner and G. Zawistowski, “Unmanned Aircraft Systems Risk Assessment Based on SORA for First Responders and Disaster Management,” *Applied Sciences*, vol. 11, no. 121, pp. 53-64, 2021.
- [9] International Civil Aviation Organization, *Convention on International Civil Aviation*, 9 ed., 2006.
- [10] JARUS - Joint Authorities for Rulemaking on Unmanned Systems, “JARUS - Joint Authorities for Rulemaking on Unmanned Systems,” [Online]. Available: <http://jarus-rpas.org/>. [Accessed 26 February 2024].
- [11] Joint Authorities for Rulemaking of Unmanned Systems, JARUS guidelines on Specific Operations Risk Assessment (SORA), Joint Authorities for Rulemaking of Unmanned Systems, 2019.
- [12] K. H. Terkildsen and K. Jensen, “Towards a Tool for Assessing UAS Compliance with the JARUS SORA Guidelines,” in *International Conference on Unmanned Aircraft Systems (ICUAS)*, Atlanta, 2019.
- [13] D. Rothe, “Development of System Architectures on the Basis of SORA in the Specific Category and Qualitative Estimation of the Implementation Efforts,” Institut für Flugsystemtechnik, Braunschweig, 2020.

# *Does combat deployment experience affect the commander's decision-making process?*

**Vladimir Statev**

Department of Military Sciences  
Vasil Levski National Military University  
Veliko Tarnovo, Bulgaria  
vladimir.statev@gmail.com

**Abstract.** The paper presents the results of a study conducted in 2022. An attempt is made to determine whether commanders' perceptions of the importance of the mission's variables change as a result of gaining combat deployment experience. A critical assessment of the mission variables is the focus of the research, which examines the importance of these variables according to the tactical commanders who plan the operations. The methods used are expert judgment elicitation and statistical analysis. The results show that combat deployment experience appears to have only a minor impact on commanders' decision-making process. The ranking list developed using the input of the experts' group, which includes officers with combat experience, may serve as a basis for improving existing models for assessing the mission variables. In order to expand the collection of research data and increase the significance of the findings, the methodology used in the study could be applied to other expert groups outside the Bulgarian armed forces.

**Keywords:** *deployment, evaluation, experience, mission variables*

## I. INTRODUCTION

The dynamically evolving security environment and the expansion of combat domains increase the degree of uncertainty in military operations. These factors negatively affect the commanders' ability to make reasonable and robust decisions. The effect multiplies down the chain of command and often has critical consequences on the tactical level of operational planning. The need for a better understanding of the decision-making process and the way experienced commanders think when planning tactical operations arises. When applied strategies fail to produce results, the usual management practice is to focus on the first learning stage – concrete experience. As a result, it is often necessary to modify the strategy itself, with the intention of transforming it into an effective management framework [1].

What differentiates a good tactical decision from a bad one is the correspondence of the conclusions made from the analysis of the mission variables, compared to the reality of

the operational environment. On the tactical level, this analysis is often done solely by the units' commanders and the success or failure of the operation greatly depends on their experience and planning skills.

The paper presents the results of a study in which two expert groups comprised of experienced military officers from the Bulgarian Land Forces give their judgment on the importance of the mission's variables when planning an operation on a tactical level. The main objective of the study is to find if combat deployment experience affects a commander's decision-making process. To achieve this task, the focus is placed on the difference in the way commanders with and without combat experience perceive the significance of the mission variables when planning an operation on the tactical level in conditions of uncertainty.

## II. MATERIALS AND METHODS

The study uses the method of experts' judgment elicitation, which is suitable for researching topics where obtaining data through measurements and experiments is hard or impossible to accomplish.

The problems associated with this type of study are the reliability of the judgment of individual experts and the appropriate number of experts in the groups. A small number of experts does not ensure sufficient statistical reliability and stability of the assessment, and individual experts have a significant influence on the aggregated results, which increases the subjectivity of the assessment [2]. On the other hand, a large number of experts in a group creates difficulties in conducting the survey. The larger the group, the lower the degree of consensus, while at the same time, the difficulty of finding a sufficient number of competent experts increases. It is generally accepted that 8-15 experts are a viable number and that the optimal number of experts should not exceed 20, as the inclusion of more leads to a decrease in the achieved results [3].

The experts are selected based on the following criteria: to have a bachelor's or higher degree in military affairs, to

*Print ISSN 1691-5402*

*Online ISSN 2256-070X*

<https://doi.org/10.17770/etr2024vol4.8196>

© 2024 Vladimir Statev. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

be an officer with at least three years of experience; and to serve in a mechanized brigade.

These criteria have to ensure that the experts have a formal education in the field of the study, have completed no less than one full training cycle of the individual to battalion-level exercises, and have done so in the units that are most rigorously trained.

Two expert groups are formed. The first is comprised of 8 officers who have at least one deployment to a combat zone (G1) and the second includes 12 who have not been deployed (G2). The experts are then asked to fill out a survey sheet that contains a table in which they have to evaluate and rank the variables taken into account when planning a mission in accordance with their importance.

The experts give each element a rank, which is an integer value from 1 to  $n$ . This way, each expert ( $Ex_i$ ) gives each element ( $E_j$ ) a specific rank ( $x_{ij}$ ). When all the experts in each group rank all the elements, the results are integrated into a matrix, as the one shown in Table 1 below. The elements presented to the expert groups for evaluation include: mission ( $V_1$ ), enemy ( $V_2$ ), terrain ( $V_3$ ), own troops ( $V_4$ ), adjacent units ( $V_5$ ), supporting units ( $V_6$ ), time available ( $V_7$ ), weather conditions ( $V_8$ ), daylight ( $V_9$ ), and anthropogenic factors not included in the other variables ( $V_{10}$ ).

When ranking the elements, all experts must use the same pre-established scale, the sum of all the ranks for each expert needs to be the same, and the experts have to give their judgment independently from one another.

The values of  $r_j$  ( $j = 1, 2, \dots, n$ ) show the sum of the ranks of all elements given by all the experts in each group, calculated using (1):

$$r_1 = \sum_{i=1}^m x_{i1}, r_2 = \sum_{i=1}^m x_{i2}, \dots, r_n = \sum_{i=1}^m x_{in} \quad (1)$$

TABLE 1 RESULTS OF EXPERTS' EVALUATION

		RANKED ELEMENTS					
		$E_1$	$E_2$	$E_{\dots}$	$E_j$	$E_{\dots}$	$E_n$
<b>EXPERTS</b>				...		...	
				...		...	
	$Ex_{\dots}$	...	...	...	...	...	...
	$Ex_i$			...		...	
	$Ex_{\dots}$	...	...	...	...	...	...
	$Ex_m$			...		...	
			...		...		
	$\bar{r}_j$	$\bar{r}_1$	$\bar{r}_2$	...	$\bar{r}_j$	...	$\bar{r}_n$

The experts rank the elements on the scale of 1 to 10 and the result of the assessment is defined by the average values of the awarded ranks which are calculated using (2):

$$\bar{r}_j = \frac{1}{m} \sum_{i=1}^m x_{ij} \quad (2)$$

When using the method of expert judgment elicitation, even with the most careful selection of the expert group, it is possible to get conflicting opinions, leading to insignificant results. The dispersion coefficient of concordance ( $W$ ) is most often used to assess the degree of agreement between experts' opinions. Its value expresses the relationship between the experts' opinions. The coefficient of concordance is a value that varies from 0 (complete discordance) to 1 (complete concordance), i.e.

when  $W = 0$ , it means that there is no relationship between the rankings of individual specialists. A value of  $W = 1$  indicates that all survey participants rank the assessed elements in the same way. The larger the value of  $W$ , the more significant the degree of confidence in the experts' evaluation results. The coefficient is calculated using (3):

$$W = \frac{12 \sum_{j=1}^n (r_j - \bar{r})^2}{m^2(n^3 - n)} \quad (3)$$

where:

$W$  – coefficient of concordance

$r_j$  – the sum of the ranks obtained by the elements in all rankings

$\bar{r}$  – the average sum of the ranks

$n$  – number of ranked elements

$m$  – number of experts

In order to interpret the resulting coefficient of concordance value of the two expert groups, the Kappa range of concordance is used [4]. It gives a clear interpretation of the results by comparing them to the scale of agreement shown in Table 2.

The calculation of standard deviation is a statistical analysis tool that allows the evaluation of the dispersion rate in the mean values of the variables generated by the expert groups. The greater the value of standard deviation the larger the dispersion and thus the intervals on the importance scale according to the experts. The small data sets allow for calculating the deviation for the entire population which is done using (4):

$$\sigma = \sqrt{\frac{\sum (X - \mu)^2}{N}} \quad (4)$$

where:

$\sigma$  – standard deviation

$X$  – the value in the data distribution

$\mu$  – the population mean

$N$  – the total number of observations

TABLE 2 KAPPA COEFFICIENT INTERPRETATION

Measurement of Observer Agreement for Categorical Data	
Kappa coefficient range	Interpretation
$< 0,00$	poor agreement
$0,00 - 0,20$	slight agreement
$0,21 - 0,40$	fair agreement
$0,41 - 0,60$	moderate agreement
$0,61 - 0,80$	substantial agreement
$0,81 - 1,00$	almost unanimous

### III. RESULTS AND DISCUSSION

Using the described methodology, the average ranks of the variables given by the expert groups are shown in Table 3 below.

The coefficient of concordance for the first group calculated using (3) is:

$$W = \frac{12 \sum_{j=1}^n (r_j - \bar{r})^2}{m^2(n^3 - n)} = \frac{12 \times 3718}{8^2(10^3 - 10)} = 0,70$$

This shows a sustainable level of agreement in the G1 experts' opinion.

For the second group, the coefficient of concordance is equal to:

$$W = \frac{12 \sum_{j=1}^n (r_j - \bar{r})^2}{m^2(n^3 - n)} = \frac{12 \times 6770}{12^2(10^3 - 10)} = 0,57$$

When compared to the Kappa coefficient range it shows a moderate level of agreement between the experts of G2.

The higher value of *W* for the G1 experts gives greater reliability to their judgment on the importance of the mission variables.

The results of the rankings are graphically depicted in Fig. 1. The darker bars represent the average ranks given by the experts who have been deployed to combat zones (G1) and the lighter bars show the importance of the variables according to the experts who have no such experience (G2).

TABLE 3 MEAN VALUES OF THE RANKINGS

Variable	G1 mean value	G2 mean value
V <sub>1</sub>	8,5	8,3
V <sub>2</sub>	9,1	8,8
V <sub>3</sub>	7,1	6,5
V <sub>4</sub>	7,8	7,7
V <sub>5</sub>	5,4	5,8
V <sub>6</sub>	4,9	4,5
V <sub>7</sub>	4,8	4,3
V <sub>8</sub>	2,5	4,0
V <sub>9</sub>	2,9	2,5
V <sub>10</sub>	2,1	2,6

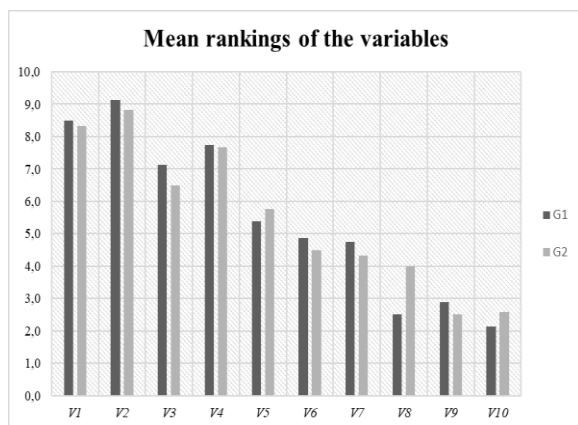


Fig. 1. Mean rankings of the variables in the planing process.

According to the experts in G1, the mission variables that are considered in the planning process are ranked by importance in the following order:

1. Enemy (V<sub>2</sub>)
2. Mission (V<sub>1</sub>)
3. Own troops (V<sub>4</sub>)

4. Terrain (V<sub>3</sub>)
5. Adjacent units (V<sub>5</sub>)
6. Supporting units (V<sub>6</sub>)
7. Time available (V<sub>7</sub>)
8. Daylight (V<sub>9</sub>)
9. Weather conditions (V<sub>8</sub>)
10. Anthropogenic factors not included in the other variables (V<sub>10</sub>)

The second group's ranking list has the following order:

1. Enemy (V<sub>2</sub>)
2. Mission (V<sub>1</sub>)
3. Own troops (V<sub>4</sub>)
4. Terrain (V<sub>3</sub>)
5. Adjacent units (V<sub>5</sub>)
6. Supporting units (V<sub>6</sub>)
7. Time available (V<sub>7</sub>)
8. Weather conditions (V<sub>8</sub>)
9. Anthropogenic factors not included in the other variables (V<sub>10</sub>)
10. Daylight (V<sub>9</sub>)

The comparison between the two lists shows very minor differences, which come in the last three positions. The most notable discrepancy comes from the perception of importance of daylight (V<sub>9</sub>) for planning operations on the tactical level. The G1 experts rate it above the impacts of weather conditions and the anthropogenic factors and the G2 experts place it at the bottom of the list as being the least significant. This indicates that the officers without combat deployment experience do not consider the limited availability, the extra weight, and the restricted field of observation of night vision sights and equipment as problematic, which is highly indicative.

Looking at the mean ranking values given to each variable by the expert groups shows that the intervals between variables placed consecutively on the two lists of importance differ by a margin of more than 10% in one of the instances. This indicates that the intervals on the importance scales of G1 and G2 are irregular and the dispersion in the mean values would be different. In order to get a numerical value, the standard deviation is calculated using (4). When applied to the data from the first expert group, the result is:

$$\sigma = \sqrt{\frac{58,093}{10}} = 2,410$$

The standard deviation for the mean values of the ranking of the variables by the second group equals:

$$\sigma = \sqrt{\frac{47,014}{10}} = 2,168$$

The difference might not seem significant at first, but when working with small data sets a rise in deviation by only 0,242 shows a higher distinction between the importance of the mission variables in the opinions of the G1 experts compared to those of G2 experts.

#### CONCLUSIONS

The results of the study show that there is no substantial difference in the way the importance of the mission variables is perceived by the commanders with and without combat deployment experience.

The substantially higher value of the coefficient of concordance of the opinions of the first expert group compared to that of the second, indicates a level of consensus among the officers with combat deployment experience. This fact gives their judgment greater credibility.

Being even marginally higher, the standard deviation in the mean ranking of the mission variables in the assessments of the first group shows greater intervals on the scale of importance from one variable to another, compared to that of the second group.

It might be argued that when pressed for time in conditions of uncertainty, commanders should focus on assessing the mission variables in the order in which they are placed by the experts of the first group.

The analysis of the data collected for the study showed that there is a difference, albeit a small one, in how commanders with and without combat experience rated the importance of mission variables and that their decision-making process was influenced by experience.

Each individual has a unique management style, expressed in their work process [5]. Officers in the armed forces are guided by the doctrines of their nations, which

affects how they analyze information and make decisions. Expanding the research to include expert groups from the militaries of other NATO countries which have similar planning processes to that of the Bulgarian armed forces would increase the significance of the results of the study.

The results and the methodology of the study may serve as a base to expand the data on the topic and to create more accurate models for the decision-making process applied by military commanders on the tactical level of operations.

#### ACKNOWLEDGMENTS

This paper 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] R. Marinov, "Dynamics in the theory and practice of the strategic management", International conference on High Technology for Sustainable Development HiTECH 2018, June 2018, Sofia, Bulgaria, ISBN: 978-1-5386-7039-2, pp 11-14.
- [2] D. Totev, "Priori ranking of evaluation criteria for the capabilities of military advisory teams and mission essential tasks for their pre-deployment training" in Collection of works "Days of Science 2014", Union of Scientists in Bulgaria - Veliko Tarnovo branch, 2014, pp. 120-132.
- [3] W. P. Aspinall and R. M. Cooke, "Quantifying scientific uncertainty from expert judgement elicitation," in Risk and Uncertainty Assessment for Natural Hazards. Cambridge University Press, 2013, pp. 64-99.
- [4] R. Landis and G. Koch, "The Measurement of Observer Agreement for Categorical Data" in Biometrics, Vol. 33, No. 1, International Biometric Society, 1977, pp. 159-174.
- [5] R. Marinov, "Styles of management for Military Security System", KSI Transactions on Knowledge Society, A publication of the Knowledge Society Institute, Volume XIII, Number 2, June 2020, ISSN 1313-4787, pp. 24-27.

# Research of the characteristics of a steganography algorithm in images when using different alphabet

Veselka Stoyanova

Artillery, AD and CIS faculty

National Military University Vasil Levski

Shumen, Bulgaria

veselka\_tr@abv.bg

**Abstract.** Steganography can be defined as a method of hiding data in cover media so that others are not aware of its existence. Steganographic systems play an important role in the covert transmission of information even in the presence of a steganalyser. The article deals with the steganography system which hides text inside images without losing data in components of RGB model. The secret message is hidden in the cover image using Least Significant Bit algorithm. The statistical characteristics of stego-images with the embedded information in Cyrillic and Latin are investigated.

The aim of the study is to determine whether there is a change in the qualitative characteristics of the stego-image, when it is hidden the same information, but was used different alphabets. The comparative results for the proposed algorithm are very promising for Cyrillic alphabet. To evaluate steganography system properties are used the measures like Signal-to-Noise Ratio, Peak Signal-to-Noise Ratio, Mean Squared Error and Structural Similarity Index for measuring.

**Keywords:** Alphabets, information hiding, Steganography, text hiding

## I. INTRODUCTION

Nowadays in the world of information technologies static and unprotected data transmission is tantamount to suicide. There are many methods by which organizations can protect themselves and to certify their right to use the transmitted confidential information. An increasingly common way to protect transmitted information is its invisibility. 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.

Steganography conceals the existence of secret information in the cover carrier [1]. Steganography can use several tapes of cover media (i.e., audio, video, image, text and network. According to [2] in Bulgaria for 2023r. 45,1% use email and 65,4% use social media or implement real-time messaging (Viber, WhatsApp,

Messenger, Snapchat, Skype, Discord, Telegram), where the main communication is realized in Cyrillic. The situation in the EU is similar, 84% users [3] have online activities of Internet. They could use mobile steganography systems or apps.

The Cyrillic alphabet to be use by approximately 250 million people. Cyrillic alphabet is the 6th most popular writing script on the planet and used across 50 languages. The Cyrillic has been the third official alphabet of the European Union alongside the Latin and the Greek alphabets [4].

## II. MATERIALS AND METHODS

### A. Basic characteristics of steganography algorithms evaluation

The stego-image characteristics of the presented LSB-based method enable its use by users in different languages around the world. This article examines and compares hidden information in Cyrillic and Latin.

The two authors from [5], tell us that the stego-file can be attacked in two ways: A visual attack and statistical attack. When we do the visual analyze we uses the human vision to detect the differences between the original object from the stego-object, whereas the statistical analyze using steganalysis algorithms based on mathematical theories [6].

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. Matlab [7] is so easy to calculate the differences between the original object from the stego-object. Ther are statistical function: *MSE*, *PSNR* and entropy. In [8] was presented the experiments in Matlab which are carried out with the fuzzy logic tool.

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8236>

© 2024 Veselka Stoyanova. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

The characteristics studied are represented by formulas (1) and (2), the PSNR is based on values obtained for the MSE:

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2, \quad (1)$$

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.

$$PSNR = 10 \cdot \log_{10} \left( \frac{\max^2}{MSE} \right) = 10 \cdot \log_{10} \left( \frac{\max}{\sqrt{MSE}} \right), \quad (2)$$

where  $\max = 255$  for 8 bit images.

The degree of similarity of the images before and after the embedding of the data, measured by the  $MSE$  and the  $PSNR$ , determines the quality the stego-image [9], [10].

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  $(i, j)$ .

$$entropy = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} p(i, j) \log \log_b p(i, j) \quad (3),$$

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  $j$ .

In Matlab we can use function to calculate the entropy:

```
I = imread('lena.bmp');
```

```
J = entropy(I)
```

In [11] is said that the most important evaluation criteria for steganography algorithms are invisibility, capacity, robustness and security. They are presented in fig. 1.

Some of these criteria can be evaluated by calculation while others can be visualized [12].

The main difference between Steganography and cryptography is that, cryptography concentrates on keeping the contents of a message secret while steganography concentrates on keeping the existence of a message secret [13].

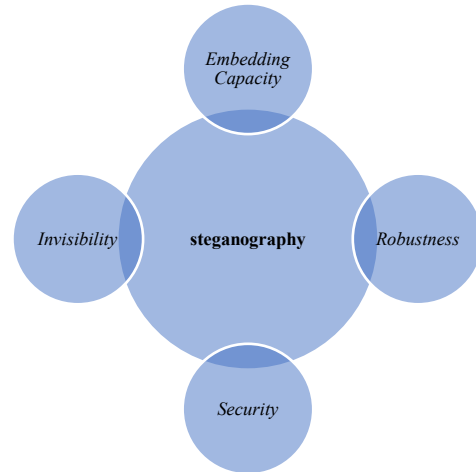


Fig.1. Evaluation criteria for text steganography algorithms

B. *Steganography algorithm based on the LSB method of embedding Cyrillic and Latin information in images.*

Least Significant Bit (LSB) replacement is the process of adjusting the most significant bits of the pixels of the cover image [10]. More details about how work LSB could be found in [14] - [19].

Proposed steganography algorithm for embedding information in images uses the last significant bits (LSB) in each color channel pixels. How this works presented on fig.2.

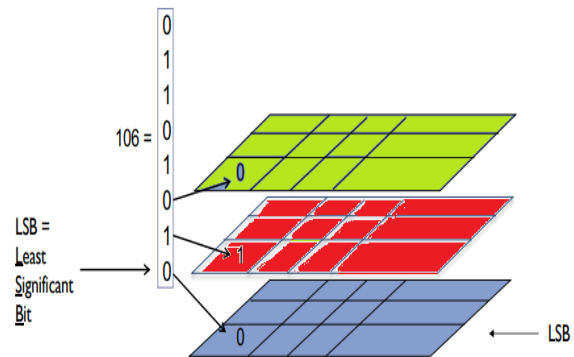


Fig.2. LSB Replacement embedding in color image

Figure 3 is a general block diagram of the algorithm, in which is checked whether there is a data entry or retrieval.

Thus is checked what operation will be realized and is proceeded to the incorporation or extraction of the confidential information. This is the main communication scheme in the steganographic environment.

The image thus extracted at the receiver's end is the same as the original image without any pixel value difference.



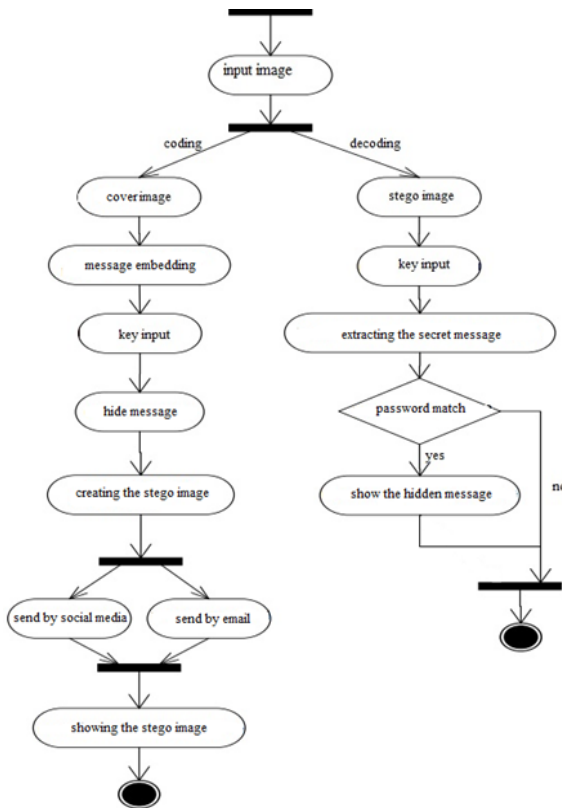


Fig.3. Communication scheme in the steganographic environment

### III. RESULTS AND DISCUSSIONS

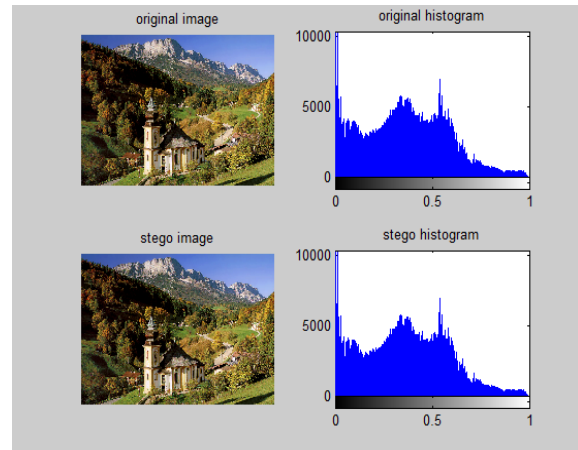
One of the main aims of the realized research of the steganography system is its practical applicability and evaluation in terms of the invisibility and size of the hidden data in the cover images. A comparison is implemented with respect to the type of alphabet used to create the secret message. Research has shown that when comparing the statistical characteristics of the same stego-images, the same secret text, but with a different alphabet, specifically Latin or Cyrillic, there is a difference in the compared statistical characteristics. On visual analysis, differences of this kind cannot be detected.

TABLE 1. HIDE 4KB LATIN AND CYRILLIC TEXT IN DIFFERENT IMAGES

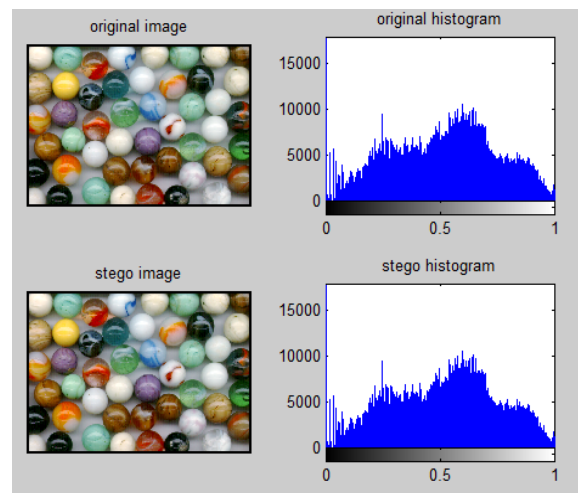
Original image	Text type	MSEav	SNR	PSNR	entropy
Alps	lat.	0.0014	62.265	69.8157	7.5557
Alps	cyr.	0.0013	62.4801	70.0309	7.5549
Paradise	lat.	0.0011	60.1414	69.8151	6.456
Paradise	cyr.	0.00098	60.1312	69.8050	6.466
change	lat.	0.0012	64.1293	69.9402	4.9676
change	cyr.	0.0015	63.8985	69.7094	4.9698
Marbles	lat.	0.0013	66.9616	72.1563	6.9900
marbles	cyr.	0.0012	67.6274	72.8221	6.9874
Ice	lat.	0.0012	61.538	69.7777	6.5832
ice	cyr.	0.0013	61.5217	69.7613	6.5833
snow	lat.	0.0012	63.5232	69.7424	7.2032
snow	cyr.	0.0011	63.5473	69.7664	7.2032
Tahaa	lat.	0.0013	64.3824	69.7678	7.7233
Tahaa	cyr.	0.0011	64.4358	69.8212	7.7232

Table 1 presents the results of the qualitative characteristics of embedded text in Cyrillic and Latin with a size of 4 kB and seven cover digital image is used. Figura 4 a) - b) and figura 5 corresponded with table 1.

In Figure 4 can be seen histograms of original and stego-image obtained by embedding of 4 kB information at base settings of the steganography algorithm, i.e. successively embedding in the three-color components of pixels without using protection by stego-key in an Alps.bmp cover image (a) and Marbles.bmp cover image (b).



a) Alps.bmp cover and stego-image

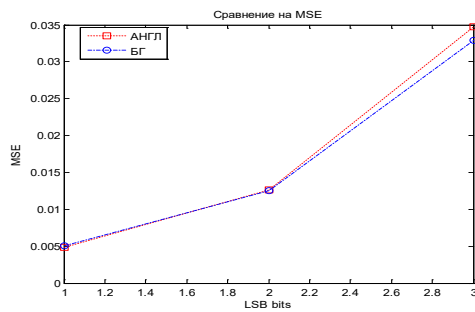


b) Marbles.bmp cover and stego- image

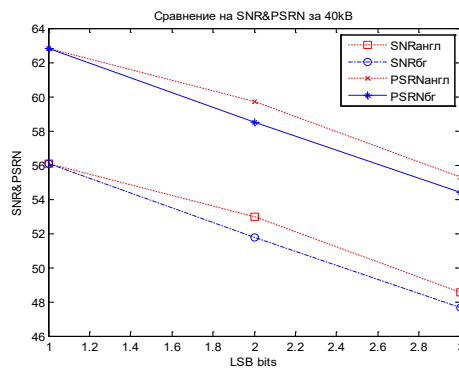
Fig.4. Histogram of original and stego-image, which has 4 kB of embedded information

This image when compared with the payload does not reveal any differences in image quality and pixels.

Table 2 presents the results of the qualitative characteristics of embedded text files in Cyrillic and Latin with a size of 22b to 2 kB and cover digital image Lena.bmp is used. Matlab compares the statistical characteristics discussed earlier in the report (1) and (2).



a)



b)

Fig.5. Comparison of hiding 4 kB information in the LSB of Latin and Cyrillic with indicators of (a) MSE и (b) SNR , PSNR by Tahaa.bmp

TABLE 2. THE RESULTS OF HIDING DIFFERENT SECRET INFORMATION IN LSB IN THE IMAGE (LENA.BMP) WRITTEN IN LATIN AND CYRILLIC

Original image	Text size	MSE lat	MSE cyr	SNR lat	SNR cyr	PSNR lat	PSNR cyr
Lena1	22b	1.3987e <sup>-5</sup>	2.5431e <sup>-5</sup>	82.5547	79.8547	87.6922	84.9923
Lena2	127b	9.7911e <sup>-3</sup>	1.7293e <sup>-4</sup>	75.0657	71.9935	80.2032	77.1311
Lena3	170b	1.4750e <sup>-4</sup>	2.848 e <sup>-4</sup>	73.1877	70.0465	78.3252	75.1841
Lena4	300	2.4033e <sup>-4</sup>	4.3360e <sup>-4</sup>	71.3278	68.1009	76.4654	73.2385
Lena5	601b	5.1880e <sup>-3</sup>	8.9518e <sup>-4</sup>	68.1496	65.0523	73.2871	70.1899
Lena6	903b	7.8837e <sup>-4</sup>	0.0019	66.3989	62.0186	71.5365	67.1561
Lena7	1.17kB	0.0011	0.0028	65.1329	60.2761	70.2705	65.4137
Lena8	1.46kB	0.0013	0.0037	64.1575	59.0956	69.2951	64.2332
Lena9	1.76kB	0.0016	0.0046	63.3459	58.1248	68.4834	63.2624
Lena10	2.05kB	0.0019	0.0055	62.6931	57.3308	67.8307	62.4684

### CONCLUSION

In this paper, detailed security analysis has been provided on the novel algorithm using visual inspection, histogram analysis, mean squared error and peak signal-to-noise measure.

The results from the research can be summarized in the following conclusions:

- A normal human being cannot identify that a sensitive data is embedded in the image independent the alphabet

- In embedding in the same image of equal length messages in Cyrillic and Latin, the stego-images obtained have approximately 0,03% difference in the values of the parameters examined and his regularity is sometimes in favor of images containing text in Bulgarian, as the percentage is almost the same.
- Difference in the histograms is hardly observed.
- When entropy values are compared in most cases no differences are observed

This result can be attributed to the fact that the embedded message is not particularly large.

### ACKNOWLEDGMENTS

The research 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] D. Artz, "Digital steganography: hiding data within data," in *IEEE Internet Computing*, vol. 5, no. 3, pp. 75-80, May-June 2001, doi: 10.1109/4236.935180
- [2] National Statistical Institute, NSI, [Online]. Available: <https://www.nsi.bg/bg/content/2823/116-лица-използващи-интернет-по-цели-на-използване>. [Accessed: Febr. 7, 2024].
- [3] Statista, [Online]. Available: <https://www.statista.com/statistics/1238307/eu-european-union-internet-users-use-accessed-internet-daily> [Accessed: Febr. 7, 2024].
- [4] B. Dimitrov, Book Exhibition Dedicated to the Day of the Cyrillic Alphabet, May 19th, 2023, [Online]. Available: <https://blogs.eui.eu/library/cyrillic-alphabet/> [Accessed: Febr. 1, 2024].
- [5] A. Westfeld and A. Pfitzmann, Attacks on Steganographic Systems. In Proceedings of the 6th European Conference on Computer Vision, ECCV 2000, Dublin, Ireland, pp. 61–76.
- [6] T.S. Reinell, R.P. Raul and I. Gustavo, "Deep Learning Applied to Steganalysis of Digital Images": A Systematic Review. *IEEE Access* 2019, 7, 68970–68990.
- [7] Image Analysis - MATLAB & Simulink, [Online]. Available: <http://www.mathworks.com> [Accessed: Febr. 1, 2024].
- [8] Kr.Slavyanov, Fuzzy Logic Procedure for Drawing up a Psychological Profile of Learners for Better Perception in Courses. In: the 12th International Scientific and Practical Conference, 2019, Vol.II, p. 140.
- [9] K. R. Rao and P. C. Yip, *The Transform and Data Compression*, 1st ed.: CRC Press, 2001
- [10] V. Stoyanova, Steganography System Using LSB Methods, ENTRENOVA. ENTerprise REsearch InNOVATION Conference, September 6–8, 2018, Split, Croatia.
- [11] T. Ahvanooy, Q. Li, J. Hou, R. Rajput and C. Yini, Modern Text Hiding, Text Steganalysis, and Applications: A Comparative Analysis. *Entropy*, 2019, 355.
- [12] M. Aman, A. Khan, B. Ahmad and S. Kouser, "A Hybrid Text Steganography Approach Utilizing Unicode Space Characters and Zero-Width Character". *Int. J. Inf. Technol. Secur*, Jan 2017, 9, 85–100.
- [13] H. Wang and S. Wang, "Cyber warfare: Steganography vs. Steganalysis", *Communications of the ACM*, vol. 47, no. 10, 2004.
- [14] A. M. Al-Shatnawi, "A New Method in Image Steganography with Improved Image Quality", *Applied Mathematical Sciences*, vol. 6, no. 79, pp. 3907 – 3915, 2012.
- [15] C. K. Chan and L. M. Cheng Hiding data in images by simple LSB substitution, *Pattern Recognition*, vol. 37, pp. 469-474, 2004.
- [16] C.C. Chang, J.Y. Hsiao and C.S. Cha "Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy", *Pattern Recognition*, vol. 36, pp. 1583-1595, 2003.

- [17] 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.
- [18] V. Stoyanova and Zh. Tasheva. "Research of the characteristics of a steganography algorithm based on LSB method of embedding information in images" *Machines. Technologies. Materials.*, vol.9.7, pp. 65-68, 2015.
- [19] E. Cole "Hiding in Plain Sight: Steganography and the Art of Covert Communication", Wiley Publishing, Inc., Indianapolis, Indiana, 2003

# Night vision monocular - basic elements and development trends

Iliya Stoychev  
Defence Institute  
"Professor Tsvetan Lazarov",  
Sofia, Bulgaria,  
i.stoychev@di.mod.bg

Iliyan Hutov  
Defence Institute  
"Professor Tsvetan Lazarov",  
Sofia, Bulgaria,  
i.hutov@di.mod.bg

**Abstract.** This article examines the fundamental elements and evolving trends in night vision monocular devices. The topicality of this topic lies in the ongoing advancements in sensor technologies, optics, and digital processing, which continually enhance the performance and accessibility of night vision devices.

The purpose of this study is to provide a comprehensive overview of the basic components and recent developments in night vision monoculars. The study adopts a comparative analysis approach, examining the key features and functionalities of different generations of night vision technology and investigates emerging trends such as miniaturization, improved image resolution, and integration with digital interfaces.

The methodology involves a thorough review of literature encompassing scientific articles, patents, and technical reports related to night vision technologies. Key aspects studied include image intensifier tubes, infrared sensors, objective lenses, and display systems. Additionally, recent research articles, technical reports, and product specifications are analyzed to identify emerging trends in monocular design and performance, in digital image processing algorithms and the integration of augmented reality functionalities.

The findings underscore the importance of ongoing research and development in improving the performance and accessibility of night vision monoculars. Key conclusions include the growing role of digital imaging in night vision devices, the potential for further miniaturization of components, and the importance of optimizing cost-efficiency without compromising performance.

In summary, this article provides insights into the foundational components and evolving trends of night vision monoculars, emphasizing the technological advancements driving the development of next-generation night vision devices. The findings contribute to a deeper understanding of the current state and future prospects of night vision technology.

**Keywords:** image intensifier, infrared, monocular, night vision.

## I. INTRODUCTION

Night vision technology has significantly advanced over the decades, revolutionizing surveillance, security, and military operations. Among the pivotal devices in this field is the night vision monocular, a compact optical instrument that enables individuals to observe low-light environments with enhanced clarity and detail. This paper delves into the fundamental components and evolving trends of night vision monoculars, exploring their historical progression, underlying principles, and future prospects.

The genesis of night vision technology traces back to the early 20<sup>th</sup> century, spurred by the imperative for nocturnal visibility during warfare and surveillance. Initial iterations relied on cumbersome infrared light sources and photocathode tubes, gradually evolving into the sophisticated electro-optical systems prevalent today. Central to this evolution is the night vision monocular—a single-eyed viewer compact enough for handheld use, embodying core technologies like image intensification and thermal imaging.

Fundamentally, night vision monoculars function by collecting ambient light or thermal radiation, amplifying the signal through electron multiplication, and presenting a visible image to the observer. This process, facilitated by advanced photonics and semiconductor technologies, has seen exponential refinement, resulting in enhanced image quality, extended detection ranges, and reduced form factors.

The contemporary landscape of night vision monoculars is characterized by a convergence of technological advancements. Miniaturization and integration with digital imaging sensors have facilitated portability and versatility, broadening the applications beyond traditional defense uses to include law enforcement, outdoor recreation, and wildlife observation.

Print ISSN 1691-5402  
Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8211>

© 2024 Iliya Stoychev, Iliyan Hutov. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

In this study, we aim to delineate the key components that constitute a night vision monocular, elucidate the underlying physical principles governing their operation, and scrutinize recent trends driving innovation in this domain. By synthesizing historical insights with contemporary developments, we endeavor to furnish a comprehensive understanding of night vision monoculars, illuminating their pivotal role in augmenting human vision under low-light conditions and outlining future trajectories for this transformative technology.

## II. MATERIALS AND METHODS

A systematic review of existing literature was conducted to gather foundational knowledge on night vision technology. Various academic databases including PubMed, IEEE Xplore, and Google Scholar were searched using keywords such as “night vision”, “night vision monocular”, “infrared imaging” and related terms. Articles, research papers, books, and technical reports published from 1990 to 2024 were analyzed to understand the historical development, fundamental principles, and current trends in night vision monocular technology.

Detailed technical specifications of night vision monoculars from leading manufacturers were collected. Specifications such as sensor types (e.g., image intensifiers, thermal sensors), resolution, magnification, field of view, spectral range, signal-to-noise ratio and weight were examined. This data was essential for comparing different generations of night vision devices and identifying trends in performance improvements over time.

Recent advancements in night vision monoculars reported in scientific journals and industry publications were reviewed. This involved studying peer-reviewed papers, conference proceedings, and technical articles focusing on innovations such as digital image enhancement algorithms, miniaturization of components, incorporation of augmented reality features, and advancements in sensor technologies (e.g., quantum dot sensors, multispectral imaging).

Quantitative and qualitative analysis techniques were employed to synthesize findings from the literature review, technical specifications, and recent advancements study. Comparative analysis was used to identify key areas of improvement in night vision monocular design and functionality.

Consultations with experts in the field of night vision technology were conducted to validate findings and gain insights into emerging trends. Discussions with engineers, researchers, and industry professionals provided valuable perspectives on challenges and opportunities in night vision monocular development.

The methodology for synthesizing and integrating diverse sources of information involved a structured approach to data collection, analysis, and interpretation. This rigorous framework ensured the reliability and validity of the study's findings.

This comprehensive approach to reviewing literature, analyzing technical specifications, studying recent

advancements, conducting data analysis, and engaging with subject matter experts formed the foundation of this study on night vision monoculars and their development trends. The insights derived from these methods contribute to a deeper understanding of the evolution and future directions of night vision technology.

## III. RESULTS AND DISCUSSION

### A. Overview of Night Vision Technologies

The primary categories of night vision technologies include light intensification (such as image intensifiers), thermal imaging, and near-infrared illumination. Image intensifiers function by collecting ambient light through an objective lens, converting it into electrons, amplifying these electrons, and then converting them back into visible light to produce a brightened image. In contrast, thermal imaging relies on detecting the heat emitted by objects, transforming thermal radiation into a visible image irrespective of available light.

Night vision devices (NVDs) are divided into two main types depending on the technology used [1]:

- NVDs operating on the principle of ambient light amplification from the visible and near-infrared (NIR) range of the spectrum and using Image Intensifier Tubes (IITs);

- Devices using the thermal radiation of the observed objects (thermal imaging technology) that operate in the IR spectrum range (3-30  $\mu\text{m}$ ). These devices detect the temperature difference between the background and the objects in foreground so they are entirely independent of ambient light-level conditions. They also are able to penetrate obscurants such as smoke, fog and haze.

There is no internationally accepted NVDs classification. For this reason, the same types of NVDs may have different names in different literary sources. Over 99% of NVDs available on the world market can be considered as models of the following species [2]:

- Night vision goggles (NVGs);
- Night vision monoculars;
- Night vision sights;
- Night vision binoculars.

The first two groups NVDs have wide Field Of View (FOV) similar to human vision (about and above  $40^\circ$ ) and 1x magnification. Two-channel NVGs allow observation with both eyes, which ensures the achievement of stereoscopic (3D) vision.

Night vision monoculars can be treated as a cheaper version of dual-channel NVGs because instead of two observation channels, there is one. Additional advantage is their small size and mass. They are designed primarily for use with one eye, resulting in reduced spatial perception. By offering portability and versatility they play a crucial role in providing enhanced situational awareness and are valued for their effectiveness.

Depending on the configuration (design) NVDs can be classified differently. The differences between the NVGs and binoculars and between monoculars and sights are small. The reason for the difference between them is

one module – the optical objective. NVGs can be easily converted into binoculars by adding afocal magnifiers or by changing objectives. Monoculars can be transformed into sights by changing the objective and adding mechanical elements allowing them to be attached to weapons.

From this point of view, NVDs can be classified as follows: bino-channel (binocular); mixed-channel (binocular) and mono-channel (monocular). (Fig. 1)

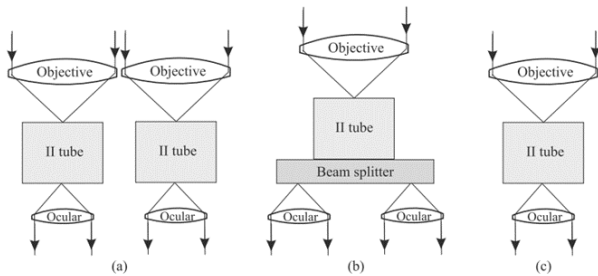


Fig. 1. Block diagrams of three types of NVDs: (a) bino-channel, (b) mixed-channel and (c) mono-channel NVDs [2].

The technical differences between them are significant and it is not possible to easily convert one type of NVDs into another.

The subject of this publication will be mainly the NV monoculars based on image intensifying technology. In fact, image-enhancement systems are normally called night-vision devices (NVDs) [3].

They are widely used in the military field to perform various tasks from nighttime field observation to tracking and surveillance. Due to its compact size and shape, this highly popular type of NVD is ideal for on-the-move target acquisition and covert operations.

#### B. NV monocular basic elements

The main structural elements of night vision monoculars well as of the other NVDs are objective lens for gathering ambient light, a photocathode tube which converts light into electrons, a microchannel plate to amplify these electrons, a phosphor screen to convert the electrons back into visible light, and an eyepiece lens for magnification and viewing. The housing of the monocular contains these components, often incorporating features like a power supply, controls, and sometimes additional optics for improved performance. These elements work together to enable enhanced vision in low-light conditions, crucial for various applications from military operations to wildlife observation [1].

The technical parameters of the device are determined by the parameters of the opto-electronic channel (objective; IIT and eyepiece). Optical systems – objective and eyepiece, are well known and used in various optical devices (Fig. 2).



Fig. 2. UL PVS-14 (NVD) [8].

#### a) Optical elements

The major requirement on a lens is a high light-transmitting function of the visible and invisible range of the IR-light. This light-transmitting function is expressed with the figures of the F-numbers (relative aperture), for instance F1.0, F1.4, F2.0, F2.8, F4.0, etc. On increasing of the figure by one, the lens is transmitting 2 times less light. A high relative aperture (lower figure of the F-number) is a very important factor for the night vision devices. The development and the subsequent production of optics with a low F-number (high relative aperture) is a very difficult and expensive task, which any company cannot easily manage. Obviously, the high costs of development and production are increasing the final price. In the race for the uninformed customers many producers are using lenses with a 3,5 up to 5 times magnification, but a low light-transmitting for long distances. It should be noticed that also two identical devices with completely similar tubes, the device with a stronger magnification would produce a lower-quality image than a device with a lower magnification. The range in the near surrounding area (residual light area) is shorter than by using a device with a lower magnification – but with a higher light transmitting.

The construction of the ocular has no impact on the range of the night vision devices, but is very significant for the observation properties. For instance, a simplification of the construction of the ocular leads inevitable to a shape-distortion of the observed object and a low resolution on the edges of the image. The oculars of some manufacturers are able to produce only a part of the whole field of view, although the tube is a major and a most valuable component of a night vision device.

Most NVDs have highly developed glass optics. The quality of devices with plastic optics is much lower than the quality of devices with solid glass optics.

#### b) Image Intensifier Tube (IIT)

What distinguishes NVDs from other optical instruments is the presence of IIT (“Tube” - Fig. 3).

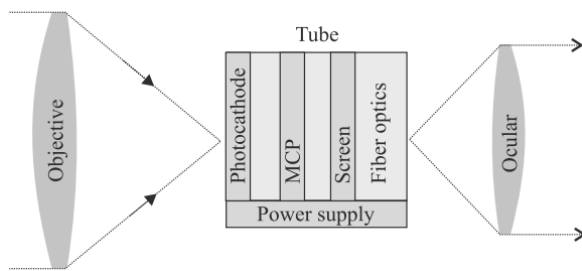


Fig. 3. Block diagram of NV monocular [2].

The objective lens capture ambient light and some near-IR light and focuses it to the photocathode of IIT, which is used to convert the photons of light energy into electrons. As the electrons pass through the tube, similar electrons are released from atoms in the tube, multiplying the original number of electrons by a factor of thousands through the use of a micro channel plate (MCP) in the tube. An MCP is a tiny glass disc that has millions of microscopic holes (micro channels) in it, made using fiber-optic technology. The MCP is contained in a vacuum and has metal electrodes on either side of the disc. Each channel is about 45 times longer than it is wide, and it works as an electron multiplier. When the electrons from the photocathode hit the first electrode of the MCP, they are accelerated into the glass micro channels by the 5,000 V bursts being sent between the electrode pair. As electrons pass through the micro channels, they cause thousands of other electrons to be released in each channel using a process called cascaded secondary emission. Basically, the original electrons collide with the side of the channel, exciting atoms and causing other electrons to be released. These new electrons also collide with other atoms, creating a chain reaction that results in thousands of electrons leaving the channel where only a few entered. An interesting fact is that the micro channels in the MCP are created at a slight angle (about 5° to 8° bias) to encourage electron collisions and reduce both ion and direct-light feedback from the phosphors on the output side [3].

At the end of the IIT, the electrons hit a screen coated with phosphors. These electrons maintain their position in relation to the channel they passed through, which provides a perfect image since the electrons stay in the same alignment as the original photons. The energy of the electrons causes the phosphors to reach an excited state and release photons. The image on the screen can be viewed directly through the ocular lens [3].

The color of the screen depends on the phosphor used. Two types of phosphorus – P20 and P43 – can be cited as the most used in modern EOP due to their high luminous efficiency. They emit light in a green-yellow color, where the sensitivity of the human eye is highest. In recent years, white phosphorus P45 has also been used, for which is claimed that the black-white image it creates is more natural to the human eye. In fact, the fatigue when observing a green-yellow image is less than when observing black and white. This effect is because the light spectrum of P20/P43 corresponds better to the light sensitivity of the human eye compared to the light spectrum of P45. It is also true that in low-light conditions, people see monochromatic images with different levels/shades of gray. In addition, users of typical NVDs

generating greenish images see the images in false colors for a certain time after removing them from the eyes. This effect is absent when using NVDs emitting black and white images. The type of phosphorus remains the choice of the user/applicant. [2]

The last element of the structure of the IIT is its output, which can be flat glass or fiber-optic plate. The fiber-optic plate (FOP) contains several million optical fibers arranged parallel to each other. Each optical fiber works on the principle of complete internal reflection. An important advantage of the FOP is that it transmits the image without loss and distortion [1].

### C. Generations [3].

NVDs are categorized by generation. Each substantial change in NVD technology establishes a new generation.

Generation 0 - The original night-vision system created by the United States Army and used in World War II and the Korean War, these NVDs use active infrared. This means that a projection unit, called an IR Illuminator, is attached to the NVD. The unit projects a beam of near-infrared light, similar to the beam of a normal flashlight. Invisible to the naked eye, this beam reflects off objects and bounces back to the lens of the NVD. These systems use an anode in conjunction with the cathode to accelerate the electrons. The problem with that approach is that the acceleration of the electrons distorts the image and greatly decreases the life of the tube. Another major problem with this technology in its original military use was that it was quickly duplicated by hostile nations, which allowed enemy soldiers to use their own NVDs to see the infrared beam projected by the device.

Generation 1 - The next generation of NVDs moved away from active infrared, using passive infrared instead. Once dubbed Starlight by the U.S. Army, these NVDs use ambient light provided by the moon and stars to augment the normal amounts of reflected infrared in the environment. This means that they did not require a source of projected infrared light. This also means that they do not work very well on cloudy or moonless nights. Generation-1 NVDs use the same image-intensifier tube technology as Generation 0, with both cathode and anode, so image distortion and short tube life are still a problem.

Generation 2 - Major improvements in image-intensifier tubes resulted in Generation-2 NVDs. They offer improved resolution and performance over Generation-1 devices, and are considerably more reliable. The biggest gain in Generation 2 is the ability to see in extremely low light conditions, such as a moonless night. This increased sensitivity is due to the addition of the micro channel plate to the image-intensifier tube. Since the MCP actually increases the number of electrons instead of just accelerating the original ones, the images are significantly less distorted and brighter than earlier-generation NVDs.

Generation 3 - currently used by the U.S. military. While there are no substantial changes in the underlying technology from Generation 2, these NVDs have even better resolution and sensitivity. This is because the photo cathode is made using gallium arsenide (GaAs), which is very efficient at converting photons to electrons. Additionally, the MCP is coated with an iron barrier, which dramatically increases the life of the tube.

Generation 4 - What is generally known as Generation 4 or "filmless and gated" technology shows significant overall improvement in both low- and high-level light environments. The removal of the ion barrier from the MCP that was added in Generation 3 technology reduces the background noise and thereby enhances the signal to noise ratio. Removing the ion film actually allows more electrons to reach the amplification stage so that the images are significantly less distorted and brighter.

There has been considerable effort expended in developing a Gen 3 tube without the ion barrier film. The effort proved successful, but the manufacturing costs were excessive compared to the performance improvements. For a brief period, the Gen 3 tube without the ion barrier film was termed Gen 4. This terminology, however, was rescinded shortly after it was announced, though some resellers of night-vision tubes still use the nomenclature [5].

In 2001, the United States Government concluded that the "Generation" indicator of an Image Intensifier sensor (IIT), be it Gen 2, Gen 3 or whatever, was not a determinant factor in an image intensifier's performance, confirming the "Generation" indicator as completely irrelevant in determining the performance of an image intensifier. For that matter, the US Government also eliminated the term "Generation" as a base for its export regulations. Instead, the Figure Of Merit (FOM) became key in determining the export feasibility [6].

FOM is easily calculated from known measured values by multiplying the values of SNR and the resolution (lp/mm) of the IIT [4].

The photocathode nowadays mainly consists of either Gallium Arsenide (GaAs), as produced by L3-Harris and ELBIT USA and against all odds still branded as Gen3 or a Hybrid Multi-Alkali (HyMa), as produced by Photonis, branded as 4G.

The main difference between GaAs and HyMa photocathodes is the bandwidth, or spectral range. In other words, the scope of types of light (from UV-blue to IR-red) that the photocathode is able to "absorb" and to transfer into electrons substantially differs. The bandwidth of GaAs is approx. 500 (blue-ish) to 900 (red-ish) nanometers. The bandwidth of HyMa is approx. 350 (UV) to 1100 (IR) nanometers. It is clear that the bandwidth or spectral range of an image intensifier with a HyMa photocathode is significantly wider than that of an image intensifier with a GaAs photocathode.

GaAs was initially thought to be a more efficient material but that was back 30 years ago (transferring light, photons into more electrons). Now it is accepted that the Signal-to-Noise Ratio (SNR) is the parameter describing how efficient the image intensifier deals with low light level. An image intensifier with a better signal to noise ratio will provide a better image in low light level condition than one with a lower SNR, irrespective of the photocathode material or "Generation".

It also became evident that the GaAs material is much more fragile, losing its essential capability quite quickly, reducing the lifetime of the image intensifier drastically. To protect the GaAs photocathode from deteriorating, an ion-barrier film needed to be installed on the MCP (that is

not required with a HyMa photocathode; all Photonis tubes are filmless) to protect the GaAs photocathode layer from ion feedback. This results in two operational consequences. First of all, it makes the image intensifiers with a GaAs photocathode extremely susceptible to laser burns, causing irreversible damages.

Secondly, image intensifiers with a GaAs photocathode results in bigger halos. Halos are round bright areas around the brightest spots in a scene, for example streetlights or car headlights, disturbing the overall image quality by 'whiting out' part or the entire image. A halo in an Image Intensifier with a GaAs photocathode would typically be around 1 mm, while the filmless 4G Image Intensifier would typically generate a halo of 0,7 mm. The smaller the halo, the better the capability to identify a possible threat (especially in urban environments). The reduced halo size in the 4G image intensifier provides clearer (less obscured) view on targets in or with light sources.

With each successive generation, the spectral sensitivity of the IIT photocathode has been shifted to an IR spectrum where the spectral density of the natural night illumination is greater than in the visible range. During the transition from the visible to the near-IR range, the transparency of the atmosphere also increases. The signal-to-noise ratio and resolution increase with each generation, as does their lifespan (Mean Time To Failure – MTTF), from 1,000 hours in the first generation to 15,000 hours in the third generation. Although of the same generation, the IITs produced by different companies differ in their parameters – resolution, integral sensitivity, signal-to-noise ratio, weight, image quality, etc. [1].

The addition of an automatic gated power supply system allows the photocathode voltage to switch on and off rapidly, thereby enabling the NVD to respond to a fluctuation in lighting conditions in an instant. This innovative function allows the observer to operate in bright ambient light, or even in daylight operations. By keeping the full capability and performance, this function provides an efficient wear-protection of the device. Furthermore, this electronic solution eliminates the glare of the light source by maintaining the performance. Moreover, this function meets the high tactical requirements - for instance by operating under bright lighting conditions such as military operations in urban terrains, which define many of today's missions. This special control electronic solution prevents blending and shadowing by variant types of light sources or fire and helps to minimize the abrasion of the tube [4].

#### *D. Development trends and innovations*

##### *a) Reduction in size and weight.*

Ergonomics (size, weight and ease of use) are important considerations. Lightweight devices are more comfortable during extended viewing. Since you will be using the device in the dark, the switches and controls should be positioned logically and be easy to use [7].

The dimensions and weight of IIT are a major factor influencing the same characteristics of NVD/monocular.

IITs differ in the nominal diameter of the photocathode. The most used in NVDs are IITs with a



diameter of 18 mm and 16 mm. The weight of the 16 mm IIT is reduced by 35 g compared to a standard 18 mm ANVIS IIT, while its volume is reduced by 40% [2].

The fatigue of the users due to the wearing of heavy NV goggles/monoculars attached to the helmet or facemask is always considered a disadvantage of NV technology. The ideal NVD should have a weight comparable to that of human eyes. Ultra-light NVDs or monoculars based on the light 16 mm IITs are a potential solution to this problem.

NV monoculars are usually offered with GEN 2+ or GEN 3 IITs depending on the user's requirements but manufacturers rarely provide information regarding the diameter of IITs used. The information in the table points to two trends – decrease in weight and increase in FOV as only the Thales product (MONIE) achieves both at a significantly shorter length than all other (>30%) (Table 1).

All models have built-in infrared illuminator as well as LED indicators for low battery and active IR illuminator. They allow focus and diopter adjustment. The presence of Manual Gain control, Bright Light cut-off, Automatic shut-off system, Automatic Brightness Control and Auto Gating depend usually depends on the users requirements. Power is provided by one battery AA or CR123 type.

TABLE 1. COMPARISON OF NV MONOCULARS.

Models	M-40, PVS-14 and similar	UL PVS-14 [8]	NVS-14 3AG [9]	MONIE [10]	MNVD-51 BRAVO [11]
Manu-facturers	Optix, AGM, ATN, Optikoelektron, EoTech, L3 Harris,	NVD	Newcon Optik	Thales	Armasight
FOV	40°/42°	40°	40°	51°	51°
Magni-fication	1x				
Weight (g)	300 - 350	235 w/o battery	287 w/o battery	< 280 with battery	310

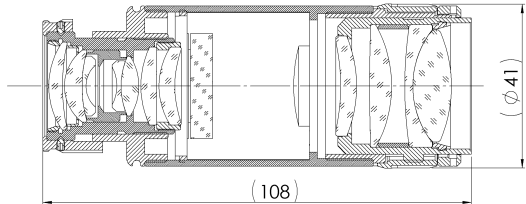
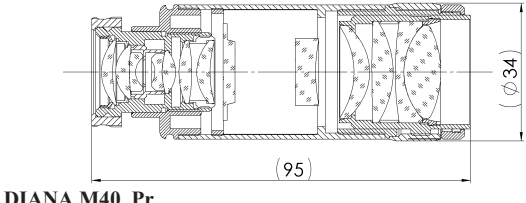
The reflection of the reduced dimensions and weight of 16 mm IIT on the same parameters of the NV monocular is shown in Table 2.

The analyses and prototype specimens show that with the use of 16 mm IIT while preserving the functional parameters of the monocular, the overall dimensions of the same will decrease by about 10% and the weight by almost 20%.

An opportunity to reduce the weight of monoculars can be sought by optimizing the construction and materials for the manufacture of the housing, as well as the optical elements of the objective and the eyepiece.

A night vision device is more attractive for the users, the smaller, lighter and the longer range it has. However, these demands are contradictory. A longer range, for instance, can only be achieved by using a device with a larger lens (diameter). The choice is finally left to the user [4].

TABLE 2. COMPARISON OF NV MONOCULARS OF OPTIX - BULGARIA WITH 18 MM AND 16 MM IITs

DIANA M40 18 mm ANVIS IIT	DIANA M40 Pr 16 mm IIT
- Magnification – 1x; - FOV – 42°; - Resolution > 64 lp/mm; - Weight – 330 gr.	- Magnification – 1x; - FOV – 42°; - Resolution > 64 lp/mm; - Weight – 260 gr.
	
DIANA M40	DIANA M40_Pr

b) Adding new functionalities.

Enhanced NVDs (dual sensor NVDs) are probably the most important trend in night vision technology. Both classical NVDs and digital NVDs suffer from the same limitation because both technologies use the same spectral band. Both devices are practically blind in dense fog, smoke, sand storms, or at very low illumination conditions. Next, these devices are also not effective against classical camouflage techniques [2].

Fusion of classical night vision with thermal imaging combines the advantages of both two technologies:

- Ability to generate high contrast images of warm targets of interest at low illumination/poor atmosphere conditions (detection task);
- Ability to generate high-resolution image of both targets and background (identification task).

Enhanced night vision goggle (ENVG) is a helmet-mounted monocular that provides the operator with significantly improved targeting and identification in all battlefield conditions and light levels. Also known mainly by the US military as AN/PSQ-20B, the ENVG uses image intensification technology fused with thermal imagery, thereby bridging the gap in performance and capability for both of these sensors (Fig. 4) [12].

The ENVG uses a proprietary mounting system due to its power supply design. The goggle does not have any onboard power. Instead, power is delivered by attaching the large 4xAA battery pack on backside of the helmet, acting as a counterweight balancing the weight of the device. There is the mounting point for the battery pack. It

is a QD design and the anchoring point matches the anchoring point on the goggle itself. ENVG powered helmet shroud has two power contacts that deliver power into the ENVG mount. Because of this, the regular helmet shroud is not usable to mount the ENVG. ENVG mount has brass contacts to deliver power to the goggle. There is one on each side so it's possible to mount the ENVG for right or left eye dominant users. The battery pack can be attached also to the side of the ENVG using the same power mounting points as the ENVG Mount. Due to the design of the housing, it is possible only to attach the battery pack to the right side of the housing. It will not fit on the left side [13][14][15].



Fig. 4. Enhanced night vision goggle (ENVG) AN/PSQ-20B (last version) [12].

Magnification is 1x and the FOV is 40° like the ordinary NV monoculars.

Enhanced Night Vision Goggle (ENVG) AN/PSQ-20 (F6023 - IIT) has high performance 16-mm image tube, 320 X 240 microbolometer, FOV -  $\geq 38^\circ$  (IIT)  $\geq 28^\circ$  Diagonal (IR) [16].

The ENVG also allows Soldiers to rapidly detect and engage targets because it permits use of existing rifle mounted aiming lights. The weight of AN/PSQ-20B is 595 grams which is identical to that of the majority of NVGs used. The system weight is about 900 grams including four AA batteries, helmet mount, and battery pack.

Next step in the development is Enhanced night vision goggle - binocular (ENVG-B) (Fig. 5) [17]. The ENVG-B is a helmet-mounted individual night vision device that has an integrated long-wave infrared (LWIR) thermal sensor and white phosphor dual IITs. The fused IITs and thermal display can be used during low and high light levels, extreme weather and with obscurants. The ENVG-B is interoperable with the Family of Weapon Sights – Individual (FWS-I) for a Rapid Target Acquisition (RTA) that provides the Soldier the ability to accurately engage targets without shouldering the weapon and execute offset shooting. ENVG-B operates on the Intra-Soldier Wireless (ISW) network with Nett Warrior (NW) allowing the Soldier to receive and display navigational, targeting, and situational graphics. It's weight is 2,5 lbs (1,13 kg). 18 mm IITs and 10  $\mu$ m thermal sensor are used [18].

In fact, it consists of two monoculars - one similar to AN/PSQ-20B and one for night image intensified vision. The significantly increased functionalities of the device in a network environment is impressive, which implies the presence of wireless connectivity.



Fig. 5. Enhanced Night Vision Goggle - Binocular (ENVG-B) [19].

According to the US Army Acquisition program portfolio 2023-2024, the prime contractors for ENVG-B are Elbit Systems of America and L3 Harris Technologies, Inc. [19].

The findings from the research carried out in this field have important implications for the design and development of next-generation night-vision monocular. Simultaneously with the work on reducing the weight and dimensions of the monocular with the use of 16 mm IIT, it is appropriate to examine the possibilities of optimizing the design of the housing, the optical elements of the lens and the eyepiece and the controls (digitalization).

The addition of new functionalities may lead to an increase in the weight and dimensions of the device, which is fully valid in the presence of a thermal imaging channel. In this case, a balance should be sought between operational and ergonomic requirements.

Due to the high weight and too high cost of devices such as AN/PSQ-20B (\$20k) and ENVG-B, it will be appropriate to explore the possibility of increasing the functionality of a regular NV monocular by providing the possibility of wireless exchange of tactical information as well as images from other devices (thermal sights or clip-on imagers for example). The cheapest and most easily achievable option is the use of a signal processing unit (SPU), probably attached to the back of the soldier's helmet, which will receive the image from the warfighter's weapon sight/clip-on imager and transmit it to the night-vision device's eyepiece through fiber optic cable. In this case, SPU can be integrated with the power source as well as to perform the role of a counterweight.

### c) Integration of AI in Night Vision Systems

AI algorithms have revolutionized night vision by enabling real-time enhancement, analysis, and interpretation of image data. The integration of AI in night vision monoculars involves several key aspects [20][21][22]:

Image Enhancement - AI algorithms can enhance low-light images by reducing noise, sharpening details, and improving overall clarity. Techniques such as denoising, super-resolution, and contrast enhancement play a crucial role in improving image quality.

Object Detection and Recognition - AI-powered object detection algorithms can identify and highlight important objects or targets in the dark. This capability is particularly valuable for military, surveillance, and law enforcement applications.

Scene Understanding - Advanced AI models can analyze night-time scenes to detect patterns, predict movements, and provide situational awareness to the user. This enhances safety and operational effectiveness in various environments.

The future of night vision monoculars is closely intertwined with AI and image processing innovations. Key development trends include:

Integration of Deep Learning Models - More sophisticated AI models, including deep neural networks, will be deployed to handle complex tasks such as semantic segmentation and anomaly detection.

Multi-Sensor Fusion - Night vision systems will leverage multiple sensors (e.g., thermal imaging, LiDAR) combined with AI to provide comprehensive situational awareness.

Real-time Decision Support - AI algorithms will not only enhance images but also provide actionable insights and decision support, aiding users in critical scenarios.

#### *d) Image Processing Algorithms for Night Vision*

In addition to AI, image processing algorithms tailored for low-light conditions are essential for optimizing night vision performance [22][23]:

Adaptive Noise Reduction - This algorithm employs advanced filtering techniques to mitigate noise artifacts inherent in low-light imagery captured by night vision monoculars. By adaptively analyzing pixel intensity variations and spatial characteristics, the algorithm effectively reduces noise without sacrificing important image details. This method enhances overall image clarity, particularly in challenging low-light environments.

Low-light Colorization - Addressing the limitations of traditional monochromatic night vision imagery, this algorithm introduces intelligent colorization to enhance visual perception. Through sophisticated color mapping techniques based on contextual analysis and scene understanding, grayscale images are transformed into color-enhanced representations. This process aids in distinguishing objects and improving situational awareness in darkness.

Dynamic Range Expansion - This algorithm extends the dynamic range of captured images, enabling enhanced visualization of both bright and dark regions within a single frame. Leveraging exposure manipulation and pixel intensity remapping, it optimizes contrast and brightness levels to reveal details that would otherwise be obscured in low-light environments. The result is a more comprehensive and realistic depiction of night scenes.

By integrating these cutting-edge algorithms into night vision monoculars, there will be a significant enhance of their effectiveness for military, law enforcement, and surveillance applications.

## CONCLUSIONS

In conclusion, this research has provided a comprehensive overview of night vision monocular technology, focusing on its fundamental components and emerging development trends. Through a thorough examination of the optical, electronic, and image intensification elements involved in night vision monoculars, key insights have been gained into the underlying principles and design considerations critical for their performance.

The study has highlighted the significant advancements in night vision technology, including the integration of digital imaging, improved sensor sensitivity, and enhanced ergonomics. These advancements are shaping the future of night vision monoculars, making them more versatile, user-friendly, and capable across various applications from defense and security to outdoor recreation and wildlife observation.

Moreover, the research has underscored the importance of ongoing innovation and research in optimizing night vision monoculars for enhanced performance under challenging low-light conditions. Factors such as resolution, field of view, weight reduction, and power efficiency have emerged as critical focal points for future development efforts.

Additionally, the study has shed light on the growing role of artificial intelligence and image processing algorithms in advancing night vision capabilities, particularly in terms of image enhancement, target recognition, and real-time analysis. AI and image processing algorithms are catalysts for the evolution of night vision monocular technology, enabling unprecedented levels of performance and functionality. The ongoing convergence of AI with night vision systems promises exciting prospects for enhanced night-time visibility across various domains. Future research will continue to push boundaries, making night vision capabilities smarter, more intuitive, and more effective in diverse operational contexts.

Looking ahead, it is evident that night vision monocular technology will continue to evolve rapidly, driven by advancements in materials science, optics, electronics, and computational techniques. This evolution promises to unlock new possibilities for night vision applications, ultimately improving situational awareness and operational effectiveness across diverse sectors.

In summary, this research underscores the dynamic landscape of night vision monoculars, revealing a trajectory of continuous improvement and innovation. By exploring both foundational elements and future directions, this study contributes valuable insights to the broader field of optical and imaging technologies, offering a roadmap for further advancements in night vision capabilities.

## ACKNOWLEDGMENTS

The authors acknowledge the support and resources provided by BDI for facilitating this study and appreciate the insightful discussions and feedback.

Special thanks to the team at OPTIX Co for their technical expertise and assistance provided by experts in night vision technology.

The authors thanks to National Scientific Program – Security and Defence for financial support under Work Package 3.1. Equipment, Task 3.1.7-Design and construction of sensor system.

## REFERENCES

- [1] D. Borissova, Night vision devices. Modeling and Optimal Design. Prof. Marin Drinov Publishing House of Bulgarian Academy of Sciences, ISBN 978-954-322- 829-4, 2015.
- [2] K. Chrzanowski, “Review of night vision technology”, Optoelectronics review, vol. 21(2), pp. 153-181, DOI: 10.2478/s11772-013-0089-3, 2013.
- [3] M. J. Haque and M. Muntjir, “Night Vision Technology: An Overview”, International Journal of Computer Applications (0975 – 8887), Vol. 167 – No.13, pp. 37-41, DOI:10.5120/ijca2017914562, June 2017.
- [4] Basic knowledge of night vision, 2020. [Online] Available: [Basic knowledge / FAQ about night vision - ALPHA PHOTONICS \(alpha-photonics.com\)](https://www.alpha-photonics.com/faq-about-night-vision-alpha-photonics), [Accessed: Feb. 27, 2024].
- [5] H. P. Montoro, ITT Night Vision, “Image Intensification: The Technology of Night Vision”. [Online] Available: [Image Intensification: The Technology of Night Vision | Imaging | Photonics Spectra](https://www.imaging-photonics.com/technology-of-night-vision), [Accessed: Feb. 27, 2024].
- [6] J. E. Weyne, Photonis Night Vision, “Differences between Gen3 and 4G image intensification technology”. [Online] Available: [Difference Gen3 4G english version.pdf \(exosens.com\)](https://www.exosens.com/difference-gen3-4g-english-version.pdf), [Accessed: Feb. 27, 2024].
- [7] T. Jacks, “The basic guide to night vision”, Thomas Jacks Ltd 2009, [Online] Available: [A BASIC GUIDE TO NIGHT VISION - Thomas Jacks - \[PDF Document\] \(vdocuments.mx\)](https://www.thomasjacks.com/basic-guide-to-night-vision), [Accessed: Feb. 26, 2024].
- [8] UL PVS-14 Night Vision Monocular. [Online] Available: [NVD-UL-14.pdf \(nvdevices.com\)](https://www.nvdevices.com/ul-14.pdf), [Accessed: Feb. 27, 2024].
- [9] NVS 14-3AG Auto-Gated Night Vision Monocular. [Online] Available: [NVS143AG.pdf \(newcon-optik.com\)](https://www.newcon-optik.com/nvs143ag.pdf), [Accessed: Feb. 27, 2024].
- [10] The lightest and most compact night vision monocular, Thales. [Online] Available: [130326 MONIE \(instigo.ee\)](https://www.instigo.ee/130326-monie), [Accessed: Feb. 27, 2024].
- [11] [MNVD-51 Gen 3 Bravo Night Vision Monocular. [Online] Available: [MNVD-51 Gen 3 Bravo Night Vision Monocular | Armasight](https://www.armasight.com/mnvd-51-gen-3-bravo-night-vision-monocular), [Accessed: Feb. 26, 2024].
- [12] Enhanced night vision goggle (ENVG) AN/PSQ-20B. [Online] Available: [Enhanced Night Vision Goggle \(ENVG\) AN/PSQ-20B | L3Harris® Fast Forward](https://www.l3harris.com/enhanced-night-vision-goggle-envg-an-psq-20b), [Accessed: Feb. 26, 2024].
- [13] C. Nicholas, Friday Night Lights: Enhanced Night Vision Goggle (ENVG) PSQ-20 B Thermal Fusion Monocular. Oct. 30, 2020. [Online] Available: [Friday Night Lights: Enhanced Night Vision Goggle \(ENVG\) PSQ-20 B Thermal Fusion Monocular -The Firearm Blog](https://www.firearmblog.com/friday-night-lights-enhanced-night-vision-goggle-envg-psq-20-b-thermal-fusion-monocular), [Accessed: Feb. 26, 2024].
- [14] Enhanced Night Vision Goggle (ENVG), AN/PSQ-20. [Online] Available: [ENVG AN/PSQ-20 - \[PDF Document\] \(vdocuments.net\)](https://www.vdocuments.net/envg-an-psq-20-pdf-document), [Accessed: Feb. 26, 2024].
- [15] Enhanced Night Vision Goggle (ENVG), AN/PSQ-20. [Online] Available: [PEO Soldier | Portfolio - PM IVAS - Enhanced Night Vision Goggle \(ENVG\), AN/PSQ-20 \(army.mil\)](https://www.army.mil/peo-soldier-portfolio-pm-iv-as-enhanced-night-vision-goggle-envg-an-psq-20), [Accessed: Feb. 26, 2024].
- [16] ITT Night Vision, Enhanced Night Vision Goggle (ENVG), AN/PSQ-20, F6023, 2009, ITT Rev. 2-09. [Online] Available: [Wayback Machine \(archive.org\)](https://www.archive.org/wayback-machine), [Accessed: Feb. 27, 2024].
- [17] Enhanced Night Vision Goggle – Binocular (ENVG-B). [Online] Available: [PEO Soldier | Portfolio - PM IVAS - Enhanced Night Vision Goggle – Binocular \(ENVG-B\) \(army.mil\)](https://www.army.mil/peo-soldier-portfolio-pm-iv-as-enhanced-night-vision-goggle-binocular-envg-b), [Accessed: Feb. 26, 2024].
- [18] Ground Systems, Binocular, Enhanced Night Vision Goggle (F6025). [Online] Available: [Night Vision - Aviation & Ground Systems \(elbitamerica.com\)](https://www.elbitamerica.com/night-vision-aviation-ground-systems), [Accessed: Feb. 27, 2024].
- [19] U.S. Army acquisition program portfolio 2023-2024. ENVG-B: “Production & Deployment” [Online] Available: [U.S. Army Acquisition Program Portfolio 2023-2024](https://www.army.mil/acquisition-program-portfolio-2023-2024), [Accessed: Feb. 27, 2024].
- [20] V. Dinesh Reddy, Sai Vishnu Vamsi Senagasetty, Krishna Teja Vanka, Mohana Vamsi Dhara, Rupini Durga Puvvada, Muzakkir Hussain, “Nighttime Object Detection: A Night-Patrolling Mechanism Using Deep Learning”, Handbook of Research on AI Methods and Applications in Computer Engineering, IGI Global, pp. 514-541, ISBN 978-166-846-937-8, 2023.
- [21] S. Singh, H. Singh, G. Bueno, O. Deniz, S. Singh, H. Monga, P.N. Hrisheeksha, A. Pedraza, “A review of image fusion: Methods, applications and performance metrics”, Digital Signal Processing, vol. 137, 104020, ISSN 1051-2004, 2023.
- [22] S. Singh, H. Singh, N. Mittal, H. Singh, A. G. Hussien, F. Sroubek, “A feature level image fusion for Night-Vision context enhancement using Arithmetic optimization algorithm based image segmentation”, Expert Systems with Applications, Vol. 209, 118272, ISSN 0957-4174, 2022.
- [23] A. Punnappurath, A. Abuolaim, A. Abdelhamed, A. Levinshtein and M. S. Brown, “Day-to-Night Image Synthesis for Training Nighttime Neural ISPs”, 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), New Orleans, LA, USA, pp. 10759-10768, DOI: 10.1109/CVPR52688.2022.01050, 2022.

# *The System Of Education, Training And Research In The Field Of Security - Managing Change Through Experience And Knowledge*

**Stoyko Stoykov**  
Vasil Levski National Military  
University, Veliko Tarnovo, Bulgaria  
Veliko Tarnovo, Bulgaria  
stojkods@abv.bg

**Abstract.** Security is a complex system of higher order, in the broad sense of the word, and represents a condition that ensures a guaranteed protection by various means of vital interests of person, society and state from any external, internal, environmental, etc. threats and they can make their progress. Security is among the basic individual and group needs that stand out independently of the cost.

Searching for and finding effective means for manageable changes in the system of education, training and scientific research in the sphere of security is crucial not only for the state's security, but for all further democratic development of the Republic of Bulgaria as a dignified partner but a source, not a consumer of security. In order to evolve in modern conditions, the system of education, training and scientific research in the sphere of security must be above all adaptive, i.e., capable of changing to respond to changes in the security environment. Change is not just one of the most important processes in one organization but an opportunity for its active and effective participation in this change.

The focus of the proposed research is on the management of specific intellectual assets and the use of the organizational channels through which knowledge flows in the security system, proposing one of the most important security policies - the transformation of the security sector - to meet the basic principles, approaches and mechanisms for the integrated functioning of institutions in the field of security - because priority threats against security require prioritized actions and reforms in investments concerning priority actions and policies due to the limited and decreasing trends of national resources. Organizational development is the study and application of practices, systems, and techniques that effect organizational change, the goal of which is to change the performance and culture of an organization.

The interrelationship and interdependence between structure, people, and procedures in the security education, training, and research system makes it imperative to follow an integrative model of organizational change that places assessment and design processes at the heart of successful organizational change

**Keywords:** change, education, management, science, security.

## I. INTRODUCTION

The security environment, where the members of the European Union want to achieve their common object, has changed radically and there are no specific security situations or threats to a particular EU country. The European Security Strategy shows that today's Europe faces new dangers that do not stop at national borders. Common solutions must be sought to address these challenges by building on the successes of the European unification process, developing what we have achieved as an expression of common security interests.

The purpose of this research is to find a scientifically based answer for the decisions in the management of the system of education, training and scientific research in the field of security, which correspond in an appropriate way with the responses of the security system to the dynamic changes in today's society. It is necessary, through the management of knowledge in the system of education, training and scientific research, to form such security for society, which meets society's expectations of stability as a guarantee of public order and sustainable statehood in the European community.

The proposed scientific study examines the design, development and functioning of the complex system of education, training and scientific research in the field of security, taking into account the peculiarities and national requirements for its organization.

## II. MATERIALS AND METHODS

### **Challenges to the national security policy**

Ensuring European security implies a serious focus on future threats and challenges - not only as identification but also as preparation of comprehensive response measures. European Security and Defence Policy, through the European Security Strategy, unequivocally shows that if Europe wants to take its share in guaranteeing global

Print ISSN 1691-5402  
Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8213>

© 2024 Stoyko Stoykov. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

security, it must have the necessary tools to fill the gaps in resources, capabilities, technology, infrastructure and to wipe out the difference between what it can today and what it would like to be able to do tomorrow. The new NATO Strategic Concept unequivocally reaffirms the close link between security and development, where the lessons from the ongoing operations show an urgent need to strengthen coordination and the need for the closest possible cooperation between political and military authorities in the planning and implementation of missions, because no member state should face the new challenges alone.

The problem of introducing the truly new, fundamental change from which we expect significant new opportunities, new horizons of development in the education, training and security research system is quite different. Continuity is the basis of the stability of traditional security organizations and is largely characteristic of the education, training and security research system. At the same time, we are facing a future full of demographic, social, economic, political, religious, philosophical, scientific and any other changes, problems, conflicts that not only appear to emerge from "nothingness" but are also accelerating, deepen, disappear or transform into one another.

The methodological framework of scientific research allows, through a comparative analysis of the studied models of change management, to derive a model that combines the ideas of the systems approach (the "transformational" cycle of knowledge assimilation and the problems of functional management are examined) with those of Kurt Lewin (based on a system concept of dynamic stability and resolution of problem situations as a tool for change management). Our capabilities are not fixed, they can be changed and upgraded because everything can be learned.

Through the transition from program-target management to comprehensive approach to security education, its advantages are pointed out as a model that not only seeks to find answers to everyday security problems, but also prioritizes improvements in the security education and training management system in the future. mindset is the secret to success in every area of life.

Today's society faces the challenge of change, and the only sure thing for the near future is that our world will be constantly changing, much more dynamically and more radically than ever.

Management is a conscious process in which the managers have previously realized and chosen the managerial impact, which is an active, planned and concrete process related to the achievement of the organization's goals. According to the functional approach, the management process is a combination of interconnected core management functions aiming to have a favourable influence on the behaviour of the system through structural change. Change management is often used in scientific circles as a synonym for transition and is a formed structured approach to organisation and system change that make it possible to move from a current to a desired future organization structure.

The challenges to national security policy arising from the existing threats and risks in the new dynamically

changing security environment imply the formulation and implementation of a new, science-based security policy and strategy for its implementation.

The problem of changes in the system of education, training and scientific research in the sphere of security and the possibility for their management is particularly relevant and at the same time very complex. This complexity results from the fact that major changes occur in all social, economic, political, group, interpersonal and personal processes, phenomena and relationships, and the external, visible manifestation of these essential changes forms the overall changes in the security system. These changes lead to new expectations and requirements for adaptability of the system of education, training and research to the dynamic changes in the security environment.

The multifaceted and rapid changes in today's integrated security environment and the need for a rapid and effective response of the security system require the structure of the main process of its activity to be a double scheme of current training. Mandatory reviews of the set of manageable variables, the formation of new strategies for their management and the detailed reporting of changes in the consequences are mandatory. This allows, on the basis of information provided and scientifically grounded solutions that security system management appropriately addresses the responses of the system to changes in the security environment.

The development and functioning of sophisticated systems imperatively require that the design and the use of management technology stems from the organization's particularities and requirements. Without a robust system of knowledge and rules for the conduct of the management operations, an efficient management process is not possible. Organizational change is inevitable, continuous, sometimes undesirable, and sometimes instigated.[1]

The first learning curve in the security system is an effective mechanism for constantly raising the knowledge in it (creating new abilities), and the second learning curve is an instrument for forming the specific new knowledge of the system.

Scientifically grounded and completely natural is the possibility of enhancing the learning outlines in the security system with the emergence of a third - "transformational learning curve" aimed at changing the context or the point of view of the system by creating a fundamental change.

### III. RESULTS AND DISCUSSION

#### **A problem of changes in the system of education, training and scientific research in the sphere of security**

Each organization is an open, dynamic, and complex system for which the main means of survival and sustainability is to maintain a state of dynamic equilibrium with the environment in which it operates [2]. The security system is presumably the most sustainable and most inert part of the public system. The whole public system relies on the stability of the security system as a major pillar of statehood, independent of political, economic and other social changes. In a period of dynamic changes, when the whole public system is reformed and transformed, the security system takes a new place, role and position in the public space, which leads to an urgent need for substantial

security changes to ensure a brand-new balance and interaction of the security system with its environment.

A balanced state security policy is possible only after a nationally responsible scientific analysis of the optimal combination without prioritization of diplomatic, political, cultural, economic and military measures in a future integrated state security sector.

It is necessary to form such a security for the society, which through a system of education, training and research, will be highly sensitive to all dynamic changes and will constantly adapt to these changes. At the same time, it must meet the public's expectations of stability as a guarantee of public order and sustainable statehood. The main efforts of the security system are focused on improving the effectiveness of the strategies for getting close to the desired results and the formation of knowledge in the training system of national security aimed at internal improvement of the expertise and increasing the efficiency of the system through the mechanisms of the applied strategy.

The first objective of the change is to ensure the selection and implementation of such characteristics of the system of education, training and security research (objectives, structure and processes) that will bring it as close as possible to the state of dynamic equilibrium. The change will create difficulties, but the lack of change creates something far worse for the organizations - entropy or gradual disintegration of the system, i.e. each organization must undergo change or cease functioning.

If new strategies are developed, the structure or technology is changed, but the conditions of people's behaviour formation in the system of education, training and security research are not changed, the first objective of change will not be realized. Every change must be realized and accepted by those who will accomplish it, which means they must change themselves. That is why the second objective of each change is to create and implement conditions for new principles of behaviour that are harmonizing with the changes in the objectives, structure and processes of the organization of the system of education, training and security research. "The central issue is never strategy, structure, culture, or systems. The essence of the problem, however, always affects the change in people's behaviour [3]."

According to its importance for the system of the education, training and security research, the organizational change can be tactical (continuous improvement within the organization) or strategic (affecting the foundations of the organization and the behaviour within the system). In the case of the pre-planned change, the system of education, training and security research will try to anticipate the future and become what it should be there. When the system does not meet the requirements of the present, the change is in the form of a reaction. Integrating changes take place within the existing objectives and strategies and are directed to maximum efficiency of processes under the conditions of moderately changing characteristics of the environment in which the system of education, training and security research operates.

The management of changes in the Learning Security System should be structured along the trajectory of the third - the "transformational" loop of knowledge acquisition. This allows the knowledge calculated in the first two contours (aimed at improving the internal operability of the system and changing its operational strategies to be accumulated as a scientific knowledge of the necessary and expected response to the significant changes in the security and defence environment surrounding the system through appropriate knowledge management mechanisms in it, modern tools to achieve the necessary - integration, flexibility, synergy, motivation and readiness for change.

Since the correspondence between strategy, structure, people and processes is never complete, the integrating changes are a continuous process, but their "power" is relatively small. Normally, organizations take well and even tolerate the integrative type of change. Everyone understands the need of them, offers options to deal with problems and acquires new knowledge etc. "For organizations that have correctly chosen their strategies according to the characteristics of the environment, integration leads to a steadily increasing efficiency and internal consistency between the strategy on the one hand and the structure, people and processes on the other [4]." Reforming changes are the consequence of major changes to the strategy, and this means that in order to implement the new strategy, changes in structure, processes and people must be made.

If the integrating changes can be called changes in the system, the reforming changes are changes to the system. An overview of scientific publications on the issue of change management shows that many change management models are derived. We will look at a model that combines the ideas of the system approach with those of Kurt Lewin (based on a systemic concept of dynamic stability and a layered process of change), in which the organization is seen as a living organism going through the following phases [5]:

- Reframe – there are determined the prospects for the development of the organization by creating an internal potential, developing an adequate set of indicators to assess the degree of fulfilment of the objectives.

- Restructure - focusing on long-term success, building a promising model of the organization by synchronizing its goals, indicators and values.

- Revitalize - looking for opportunities for development and growth by focusing on the requirements of applicants, consumers and the market.

- Renew - encouraging the creation and dissemination of new knowledge and skills in the organization. Stimulating individual training, developing the organization and educating employees to a sense of belonging to it.

Organizational change is a specific type of change that affects the nature of the processes, the structure, the systems and the way they are managed. It is the basis of the organizational development. It resolves not only the problems of external adaptation, through restructuring and strategic planning, but internal integration as well as - by means of introduction of new values into the organizational culture. Organizational change management is a planned

process that aims at achieving higher levels of organizational effectiveness.

Structural change in the context of organizational change refers to the improvement of activity through changes in the officially adopted structure of relations between tasks and power. At the same time, it must be acknowledged that the structure creates interpersonal and social interactions, which can gradually become decisive for academic activity.

The internal connection and interdependence between the structure, people and procedures in the education, training, and security research system must be known and understood. Many specialists emphasize that less effort is being made to change if it focuses only on the structure, or only on people, or on procedures alone.

The integrative model of organizational change puts assessment and design processes at the core of the organizational change. Changes in people are principally focused on knowledge and skills expansion – i.e. to make a change through competence management in the system of education, training and security research. Lifelong learning is crucial for introducing changes in human resources into the system of education, training and security research, and in many cases this training should be differentiated from the "traditional" one [6].

This does not mean that we should not conduct preparatory research and try to assess and minimize the risk, to plan, program and prepare the introduction, create conditions, and try to predict and overcome the problems in changing the system of education, training and security research through balance of change and continuity.

Security organizations and their individual employees have their own unique goals, values and expectations, and there is usually an area of overlap where their goals are common. When the organization introduces a change, the overlapping area moves. The goals, values and expectations of the organization are changing, creating a potential conflict for individual employees, and their resistance is a natural and normal response to change. And this is a very human reaction to falling into new or unknown circumstances.

The knowledge-based security strategy - a comprehensive approach to security education

Modern requirements for education in the field of national security require extensive increase of knowledge according to the adopted national security system of the country. In addition to purely national elements, which are security-related, they include elements of NATO and EU allied defence, too.

Often, the results of the scientific and educational activity in the security system remain hidden for society, which inevitably leads to a separation of public opinion regarding the importance of the objectives pursued and the public resources allocated to them. Criticisms of our education system will not spare education in the security system, without taking account responsibilities of each one of us to the security of the country, because social development can cause irreparable damage and create new threats and confrontation between different socially

significant groups (teachers, doctors, policemen, miners, military, retirees).

The management of large organizational systems, such as the security system in its historical development, is related to the progress of system management and the approaches and concepts developed by it. Solutions at different hierarchical levels in the security system are confronted through the choice of alternative actions with different effects on threats and security. The cost of resources for the chosen alternative is also different. The effectiveness of management is largely influenced by the type of management constraints and the decisive power of the analytical apparatus linking the effects and costs of management.

It is imperative in solving theoretical, methodological and practical issues of the effectiveness of management of organizations to consider both the management itself through indicators of organizational effectiveness and its effectiveness. The problem of the efficiency of the functioning of the management systems of the complex systems is complex, multifaceted and therefore is decomposed into several main subproblems. Factors that affect the efficiency of a complex system can be divided into two types: internal and external.

The effectiveness of the management of an organization reflects the relationship between the set management goals, the existing conditions, the effects of the activities of the management entity, the final results of the organization and the resources expended.

Efficiency is one of the main evaluation concepts of the organization's management and is a complex concept, which is determined by many factors related to two concepts: economic efficiency, reduced to determining the size of management resources in terms of management effects and social efficiency, determined through the obtained effects of a social nature. Properly formulated management of each organization must ensure an optimal combination of these two types of efficiency, which are mutually determined.

The effectiveness of the functioning of any complex organization is directly dependent on the correctly formulated policies and their implementation in the existing management system. The problem of improving the management systems of organizations in solving the task of creating new and opening and mobilizing existing reserves using the available resources in organizations is becoming increasingly important.

But the functions of the elements are subject to the speed and dynamics of the changing structure of the organization. There is a contradiction between the rapidly changing goals and the more static and structure-related functions. The solution to this problem, as far as possible in functional organizational management, leads to the search for and development of multifunctionality. The practice requires the exclusion of duplication of functions, high integration and efficiency of functions, allowing rapid suppression or development of new functions if necessary. The growing integration of management functions does not provide a solution to the main contradiction of functional management. The discrepancy between the changing environment (and goals) and the adequacy of the actions of



the functional system can be largely overcome by the transition to program (progra-target) management.

The need for a comprehensive approach to security education seems unquestionable, but it requires a model that seeks not only to find answers to the day-to-day issues, but to prioritize improvements to the education management system and security training. An advanced improvement in governance of educational institutions in the security system will allow the discovery of talented people who are experts in decision-making and are capable of taking responsibility. Awareness of our own creativity will bring full satisfaction for the efforts made in the formation of new and clearly necessary knowledge for the future. Security knowledge is compared to the wisdom gained throughout the centuries from the society, through the use of different instruments to achieve its unity and community, because "science-wisdom is knowledge of origin and causes.

In order to achieve higher quality of education and training in the security system, traditions and continuous training of teaching staff, large volumes and diverse teaching materials, skilful compilation, coordination and maintenance of complex plans and programs are needed, creating conditions for formation of knowledge for security in their completeness and interdependence.

The security system will not be able to maintain its function of supporting the statehood in society, if it didn't reflect these changes, problems, conflicts and don't act in accordance with the requirements of each specific moment of these processes and their concrete manifestation within a certain range. It will not be a reality if the relevant organizations in the system of education, training and security research are not constantly changing in order to meet this future [7, 8].

The choice of an alternative for change is based on the comprehension of the essence of the problem for the organizations in the system. And at the same time, it is also influenced by the concrete conditions under which change is made.

Changes in the system of education, training and research into security through "organized improvement" and "exploitation of success" are small successive steps away from the result for a better and wider outcome. In this sense, they do not need special means of introducing beyond the usual ones, namely: the introduction of new administrative products and services, as well as the necessary new techniques and technologies, the training of people for their absorption and application, a gradual change of functions and how these functions are performed. The choice of an alternative for change is based on the comprehension of the essence of the problem for the organizations in the system. And at the same time, it is also influenced by the concrete conditions under which change is made.

The main factors determining the outcome of change management efforts relate to the three types of organizational change in the system of education, training and security research: structural change, change in human behaviour and change in technology and procedures of education and research. Each of these impacting factors can become the focus of the effort for change. What is

important in this case is that the change in each of the factors is in line with others, for example a change in the mission-oriented security system leading to the closure of formations and infrastructure contradicts the traditionally sustainable labor relations which must obligatorily exist in the security system.

Knowledge management in the security system encompasses various management tools related to the concepts of intellectual capital management and the idea of a learning organization, including the creation of professional communities, using intranet systems, document management systems, and wiki-based systems [4, 10]. The focus on the management of specific intellectual assets and the use of organizational channels on which knowledge is flowing is that which distinguishes security management knowledge programs in the security system from continuous organizational learning initiatives.

The knowledge-based security strategy should propose and outline one of the most important security policies - the transformation of the security sector by responding to the basic principles, approaches and mechanisms for the integrated functioning of our institutions [3, 11]. Priority threats require prioritized actions and reforms in the investments, concerning priority actions and policies due to the limited and decreasing trend of national resources.

In the security system where there is a high degree of subordination, the people change speed is extremely slow. Organizations in the system of education, training and security research are doomed to be "moderate leaders of change" that create, retain and continually restore the balance between the continuity that is inherent in every state and the changes imposed by the accelerating social time. Peter Drucker sees the solution in the slogan: "Let's change together" and there's probably a good reason of this.

## CONCLUSIONS

The dynamics in the development of modern security risks and threats have changed the main components of the modern security environment and the achievement of a balanced state security policy, as a priority objective is possible only after a nationally responsible analysis, optimal combining without prioritizing diplomatic, political, cultural, economic and military measures in a future integrated state security sector. National Security Policy is a set of mutually related priorities and sectoral policies that are on an equal footing, and their role and place in specific situations and periods is determined by the dynamics of the security environment and the necessary actions for the realization of the national interests.

In order to change the organizational culture in the system of education, training and security research, action is needed, not just slogans and spells to change values. These are specific modifications to the strategy, structure and procedures that lead to system development rather than vice versa.

Now, processes of consolidation of the educational system are underway in the Republic of Bulgaria, during which the opinions of specialists in the field of military education are wanted. In this way, the idea of change does not remain only an idea but is implemented in practice through my inclusion in a working group of the Ministry of

Education and Science from the beginning of 2022 and the opinion submitted by me regarding the work of the academic staff, the scientific training of the academic staff, the scientific achievements of the academic staff, as well as its assessment. In the opinion, I also noted the importance of supporting the academic staff for outstanding achievements of a scientific and practical nature in the field of security and defense.

By the end of 2022, it is expected that the change in the law on the development of the academic staff in the Republic of Bulgaria will be developed and adopted.

Now, in the Republic of Bulgaria, the change I am talking about, which is based on competences, is beginning to take place through the necessary change in the legislation regarding laws and regulations for the development of the academic staff, and specifically in the field of security and defense. Military education in Bulgaria needs a common basis, an understanding between the higher military universities and academies, common and synchronized curricula, on which to stand and stably build the future training of its cadets and officers.

#### REFERENCES

- [1] E.Petrova, Management in the Changing World. Veliko Tarnovo, Publishing Complex of the Vasil Levski National Military University, 2012.
- [2] E.Petrova, Management in the Changing World. Veliko Tarnovo, Publishing Complex of the Vasil Levski National Military University, 2012 .
- [3] Kotter, John., St. Cohen, The Heart of change. Classic and style. Sofia, 2003.
- [4] V.Vasilev, Effective public management. SWU Neophyte Rilski. Blagoevgrad 2011.
- [5] K.Lewin, Group decisions and social change. Swanson, G. et al. Readings in Social Psychology. Holt, Rhinehart & Winston, 1958 .
- [6] V.Dimitrova, The impact of coaching on the Emotional Intelligence of Managers in the Organization, International Conference on Creative Business for Smart and Sustainable Growth (CREBUS), Sandanski, INSPE, 2019..
- [7] R.Marinov, Dynamics in the theory and practice of the strategic management. International conference on High Technology for Sustainable Development HiTECH 2018, 11-14 June 2018, Sofia, Bulgaria. Date Added to IEEE Xplore: INSPEC 2018.
- [8] 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
- [9] 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; <https://doi.org/10.1108/978-1-83753-190-520231004>, 2023
- [10] D.N.Todorov, State of the population disclosure systems in the changing radiation situation in Bulgaria, Vide. Tehnologija. Resursi - Environment, Technology, Resources, 2019, 1, pp. 54–58
- [11] HGigauri, I., Vasilev, V.P. .Paradigm shift in corporate responsibility to the new ERA of ESG and social entrepreneurship; Book Chapter: Sustainable Growth and Global Social Development in Competitive Economies, pp. 22–41; [https://www.igi-global.com/gateway/chapter/330086?fbclid=IwAR3JMbgGR8RvOnw3P7QsSIh6vwpZnjUV0QkYlrh0W7Cy2Pzt-H\\_kzBp50AI](https://www.igi-global.com/gateway/chapter/330086?fbclid=IwAR3JMbgGR8RvOnw3P7QsSIh6vwpZnjUV0QkYlrh0W7Cy2Pzt-H_kzBp50AI); DOI:10.4018/978-1-6684-8810-2.ch002, 2023

# *Trends in the development of modern international relations. The new challenges for diplomacy*

**Plamen Penkov Teodosiev**

*Department of National Security,  
Faculty of Information Sciences,  
University of Library Science and  
Information Technology  
Bulgaria  
p.teodosiew@unibit.bg*

**Abstract.** The report analyzes the modern international system and the factors that influence its development. The impact of the Great Powers, the development of information technology and the impact of social media on the dynamics of international relations are considered. The imbalance of the system, provoked by the fundamentally different views of the main actors - the United States and Russia on the main issues, has increased over the years due to the lack of dialogue aimed at finding mutually acceptable conditions for its existence. There is an aspiration for multi-regionalization of the international system and the emergence of new "players" – China, India, the United Arab Emirates, Saudi Arabia and the Republic of Türkiye, which seeks to acquire the role of a regional balancer, including through existing regional conflicts, and in the Balkans to be a regional leader. The mosaic of modern international relations is characterized by the restructuring of connections within existing subsystems, which inevitably affects the degree of entropy of the entire system and its individual elements.

**Keywords:** international system, international relations, national identity, social networks, global and international security, diplomacy

## I. INTRODUCTION

The dynamics of the processes affecting the architecture of the modern system of international relations are unprecedented in historical terms. Digitalization, globalization, growing status in the field of technology and production (the approaching "cyber wave" of the scientific and technological revolution), the highly active phase of the rise of several civilizations provoke multi-level rivalries between states that rightly view "periods of crises as a time of opportunity". The limited possibility of long-term planning under these conditions

affects the stability of alliances, which means high instability in the problems of determining the "balance of forces" and the "balance of threats". And as a normal development is the aspiration for multi-regionalization of the international system and the emergence of new "players" – China, India, the United Arab Emirates, Saudi Arabia, the South African Republic and, to some extent, Turkey.

China, a country that in recent years has established itself as one of the world's economic powers, seeks to be a leading factor in both the UN and global political and economic alliances – BRICS, SCO and G20.

India, which has recently sought to catch up with China in terms of economic growth, has become an informal leader among the countries of the South Asian Association for Regional Cooperation (SAARC).

The United Arab Emirates and Saudi Arabia, following the change in generations governing the countries, became the informal leaders of the countries of the League of Arab States (Arab League) and the Organisation of Islamic Cooperation (Islamic Conference).

Türkiye, which aspires to play the role of a balancer in regional conflicts and a regional leader in the Balkans and among Turkish-speaking countries, but due to the ambivalent and controversial policies of the country's president, RT. Erdogan is not perceived positively by both the West (the European Union) and Arab countries.

The mosaic of modern international relations is characterized by the restructuring of connections within existing subsystems, which inevitably affects the degree of entropy of the entire system and its individual elements – the struggle for leadership and supremacy, the growing

*Print ISSN 1691-5402  
Online ISSN 2256-070X*

<https://doi.org/10.17770/etr2024vol4.8207>

© 2024 Plamen Penkov Teodosiev. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

importance of nation states, the struggle for control over natural and energy resources, the struggle for influence over postcolonial states in Africa and Latin America, the rise of the "power factor" in international relations, hybrid and information wars, the decrease in the importance of the UN Security Council, etc.

The modern system of international relations is still in the process of conceptualization and given the complex mosaic, the crisis component can hardly be defined at the moment

## II. MATERIALS AND METHODS

### **2.1. Reducing the role of the UN in the system of international relations**

With its establishment after World War II, the United Nations (UN) was called upon to become not only a universally recognized regulator of international relations but also to establish itself as an international institution that could unite the efforts of all countries to build a just and free world, assisting in solving the most important political and socio-economic problems of humanity and being adequate to the new geopolitical realities.

In the first years, however, the world was divided into two warring 'camps,' with the leaders of these countries—the United States and then the Soviet Union (now Russia)—being veto-wielding countries in the UN Security Council, the body empowered to make adequate decisions to quell these conflicts. The fact is that most conflicts violate the interests of some of the leading states in the Council. [1]

In line with the global opposition imposed after World War II, it can be pointed out that international law takes on a special role. The establishment of certain rules of conduct of the blocs, both vis-à-vis each other and vis-à-vis third countries and regions, the interpretation of international law, and, above all, its generally recognized norms, allow for the strategic initiative to be taken (and withdrawn) and for rules of conduct to be dictated on the world stage in a peaceful manner, even playing a rather substantial propaganda role.

Within the framework of modern conflicts, the presence and active development of international law allows entry into the foreign information space and erosion of the basic values of the enemy camp – imposing or attracting in its rank's supporters of "respect for human rights" or, respectively, opponents of "world imperialism". As a result of these trends, a set of fundamental principles of international relations has formed in the UN system. As a result, after the end of the era of block opposition, today only the World Organization has the necessary legal basis and generally recognized legitimacy that allows it to act on the international stage as an expression of the interests of all countries and people. In this context, it can be noted that interpretations of international law as the primary regulator of relations between states are somewhat exaggerated. This is especially evident in the analysis of the contemporary processes of the major world communities, which are less and less inclined to absolutize international law and, accordingly, the UN as a

major international institution guaranteeing the inviolability of the basic principles and norms of the global international system.

If we assess the international situation since 1946, more than 90 wars have been fought in the world, and the total number of conflicts, including internal ones (Kosovo, Bosnia and Herzegovina, Israel) is about 400. This leads to the conclusion that this trend objectively reflects the existing political and socio-economic contradictions of different communities, from local to national (ethnic) and religious to regional. In this regard, international law, as a system for regulating international relations on the one hand, and the UN as the only and global institution ensuring its implementation, are derivatives of various factors (military, political and socio-economic). It can therefore be said that international law and the UN are not stand-alone and self-sufficient factors in international policy regarding conflict resolution. In modern conditions, interpretations of international law and the establishment of the UN are the result of post-war regulation and reflect specific historical conditions. In accordance with the already imposed and necessary changes in the world order, need a very substantial transformation of the modern system of international relations, which requires a revision of the basic norms in international law and the regulations on the status and activities of the United Nations.

If we illustrate the UN with a large corporation, then there are always complex vertical and horizontal links between the individual structural units, and as a result, vertical integration, i.e. the construction of a link between the individual units, remains incomplete. The main office (for the UNSC case) has too many functions and responsibilities and in this regard has too much information to be able to take operational and adequate decisions in a particular situation. At the same time, the governing body of the corporation is not aware of what is happening in the structural units located below it and in this regard is not able to exercise control over the decisions already taken. This leads to a management crisis that leads to the removal of the corporation and the conquest of markets by its competition. In order to overcome such a situation, there are no other solutions in management practice, except to transfer some of the functions and the main responsibilities for their implementation.

### **2.2. Economic organizations in the world**

In the Americas, the North American Free Trade Agreement (NAFTA) was established, replaced as of July 1, 2020 by the United States-Mexico-Canada Agreement (USMCA), Caricom, Caribbean Community, Parlacen, Central American Parliament, Andean Community, Andean Community, Mercosur, Mercosur, Trade and Economic Bloc of South America.

The European Union (EU) and the European Free Trade Association (EFTA) have been established in Europe

In Africa, Arab Maghreb Union, Union of the Arab Maghreb, Economic Community of West African States (ECOWS), Economic Community of West African States, Central African Economic and Monetary Community (CEMAC), Central African Economic Community, Intergovernmental Authority on Development (IGAD), Intergovernmental Development Authority, Southern African Development Community (SADC), Community for the Development of Southern African States were established.

In Asia there are Commonwealth Independent States, Commonwealth of Independent States (CIS) and South Asian Association for Regional Cooperation (SAARC), Association for Regional Cooperation in South Asia.

The Association of Southeast Asian Nations (ASEAN), Association of Southeast Asian Nations and Pacific Islands Forum, Pacific Islands Forum are structured in the Pacific region.

The Gulf Cooperation Council (GCC), the Gulf Cooperation Council, operates in the Middle East.

### **2.3. Political alliances in the world**

Part of the Economic Intergovernmental Authority for Development, Southern African Development Community (SADC), the Southern African Development Community, The Association of Southeast Asian Nations (ASEAN), Parlaten, the Central American Parliament, Mercosur, Mercosur, the trade and economic and political bloc of South America, Europe and the United States are represented by the North Atlantic Alliance NATO, the Arab countries of the Arab League, the Arab League, some of the Asian countries and Russia are in the Shanghai Cooperation Organization, Shanghai Cooperation Organization. The latter is gaining more and more popularity after the crisis in Ukraine and could become one of the leading mediation organizations in its attempt to resolve regional conflicts.

BRICS, whose abbreviation is made up of the five founding countries – Brazil, Russia, India, China and South Africa, is also becoming a leading political and economic union. At its last meeting in South Africa, the organization decided to be joined by six more countries – Saudi Arabia, Iran, the United Arab Emirates, Argentina, Egypt and Ethiopia.

Organisation of Islamic Cooperation (OIC), established as Organisation of Islamic Conference and renamed in 2011. It includes 57 countries from the Middle East, Africa, Central Asia, the Caucasus, the Balkan Peninsula, Southeast Asia, South Asia and South America.

African Union, African Union. An economic organization uniting 55 African countries.

### **2.4. The struggle for leadership and the modern world order**

The dynamics of the processes affecting the architecture of the modern system of international relations are unprecedented in historical terms. Digitalization, globalization, the development of scientific technologies and new industries (the approaching "cyber wave" of the scientific-technological revolution and the

advent of artificial intelligence technology), the highly active phase of the rise of several countries, such as China, India and to some extent Türkiye, provoke multi-level rivalries between the great powers and the new "players". The limited possibility of long-term planning under these conditions affects the stability of alliances, which means high instability in the problems of determining the "balance of forces" and the "balance of threats". The mosaic of modern international relations is characterized by the restructuring of connections within existing subsystems, which inevitably affects the degree of entropy of the entire system and its individual elements.

For example, one of the characteristic features of such a process is problems that are 'old' in form but have acquired 'new' content in the current context, among which religious and ideological conflicts stand out. The modern system of international relations is still in the process of conceptualization, but its crisis component can be identified now. After the fall of the "Berlin Wall" and the subsequent collapse of the Soviet Union, which led to the end of the bipolar system. The balance of power has changed, there has been a transformation of certain principles of interaction, but the common ground, the spirit and the institutions of the Cold War continue to exist today. The concept, which is also often characterized as multipolar, presupposes the evolutionary development of existing institutions of global political stability, while preserving the specifics of the structure and functioning of sovereign nation-states. On the one hand, the United States and Western European countries insist on the unification of the world order on the basis of their own model of civilizational development, demanding reforms from partners in the economic, political and social spheres as a prerequisite for cooperation. To achieve their goals, in some cases they even demonstrate a willingness to ignore the existing international legal norms and institutions of global governance, but the practice of international processes at the moment shows the impossibility of forming uniformity for longer than "momentary" time. At the same time, Russia, the United States, China, India and the developed Arab countries are expressing positions for the formation of different forms of polarity, even for the formation of a lack of such polarity. This theory does not seem completely devoid of meaning in the context of the growing chaos and anarchism in the international arena over the last few years. Even among the "great powers", there is a decrease in the desire to expand their area of responsibility beyond the obvious boundary spaces and consolidate tendencies to concentrate on one's own problems in various forms of isolationism.

The imbalance of the system, provoked by fundamentally different views of its key elements of the basic actors - China, Russia, the United States, has deepened over the years due to the lack of dialogue aimed at finding mutually acceptable conditions of existence. The confrontation went from direct to propaganda campaigns supported by levers from a broad toolbox of 'soft power' and to the most utilitarian adoption of this concept, including the use of elements of the extremist and terrorist spectrum, which, according to some authors, have become 'legitimate means of policy-making'. In such circumstances, one of the most pressing issues of modern

foreign policy is the problem of 'proportionate response'. On this basis, discussions on modern concepts of war have arisen in expert circles. As a result, today such concepts as "proxy war", "hybrid war" are only a reflection of reality, where the main actors seek to lower the threshold for the use of weapons, avoiding a direct clash between nuclear powers. [2]

Contrary to hopes, the collapse of the bipolar system (the dissolution of the Soviet Union) did not lead to a decrease in global conflict. The dynamic change in global transformations is forcing global players to develop new supranational platforms and decision-making mechanisms whose procedural functionality is adequate to the changed realities of the international scene. Through their projects, the Eurasian Economic Union, the Asian Infrastructure Investment Bank, the Shanghai Cooperation Organization, the BRICS, the Gulf Cooperation Council, etc. in certain regions where their activities correspond to the relevant international subsystems. In this way, the regionalization of international relations is being updated to some extent, and the importance of the elements of the global system is increasing due to more stable and reliable connections in the distributed spaces. Additional homogeneity of the subsystems is given by the conflicting interaction in the periphery, in the area of their "contact", where individual subjects of world politics are objects in the game for markets and zones of influence between different centers of power. The most stable subsystems are characterized by the presence of a "leader" around which the consolidation and integration of the region takes place. By building their own inclusive security system in the region, including imposing border restrictions and establishing economic cooperation with neighbouring countries, such leaders may in the future achieve the level of a 'great power'. The formation of new power centers is a natural consequence of filling the vacuum created after the breakdown of the system by two equivalent poles regulating the space around them. One of the most significant aspects today is the opportunity to offer the world new ideas and ways of development. In this regard, for example, China's ideological and economic path is attractive; but Western democracies are becoming vulnerable as a result of huge migrant pressure, weakening the social system and creating risks of a new wave of terrorism. Regional 'powers' such as Turkey and India are also emerging, seeking to become a key factor for security and, in general, for the international system. Russia, which has relied on state interests throughout the post-Soviet years, faces the need to develop micro- and macro-ideas aimed at both developing its own nation and achieving peace, which implies at least strengthening humanitarian cooperation, mainly with the former Soviet republics and the "Russian world" (part of the former socialist republics, including Bulgaria).

Following the decision of the last BRICS meeting held in 2023 in South Africa to join six more countries, the organisation will represent around 46% of the world's population and generate 37% of the world's gross domestic product (GDP) [3]. With its current composition,

BRICS generates 24% of global GDP and represents 42% of the world's population.

The intensification of the ideological factor in the world system influences the frequency and scale of the spread of radical concepts based on fundamentalist aspirations appealing to the idealized past, which are generally based on the ideas of intolerance and the definition of an "external enemy". The fight against fundamentalism consumes too many resources and causes a spillover from one radical group to another. Such is the case with the formation of the Islamic State terrorist group, Kurdish separatist movements, Hamas, etc. The strengthening of this trend is facilitated by the policy of the United States, which, testing its own foreign policy development (the concept of controlled chaos), as well as due to a misunderstanding of the specifics of the political process in the East, provoke the collapse of regional systems. On the other hand, Russia, in order to counter these American aspirations and to divert conflict points from its own territory, is controlled to support "anti-terrorist groups", whether legitimate or opposition governments. The determining factor in this case is the socio-economic situation of the population, which due to a serious demographic "youth bulge", high unemployment, difficult economic conditions has been influenced by the preachers of radical ideologies.

### **2.5. The specifics of national identity in the global world**

Nations are under considerable pressure from migratory flows, which lead to the erosion of consciousness, traditions and the state as an apparatus for managing society [2]. The consequences of the clash of interests of different structures go far beyond the regions in which they occur. The number of potential and actual conflict zones where, due to a careless step by the authorities or a tactical move by extra-regional players, an acute internal political crisis spilling over into civil war may flare up as interdependence and mutual openness in the regions grow. As a result of geopolitical transformations, and often catastrophes, countries that are actually the apparatus for population management arise and disappear. A state can be formed, but that does not mean that a nation is formed. At the same time, the nation is the key to a strong and successful state. Nation-building is a complex, multi-stage project. Its ultimate effectiveness depends on the will of the people and the competence of the state governing bodies, which systematically through ideological content and the creation of favorable external conditions can contribute to the construction of the nation. Thus, the formation of a nation will have positive dynamics and a result only within the framework of the simultaneous movement from the bottom up and from the top down. It seems impossible to build a nation relying solely on administrative resources, without a willingness on the part of society. A distinction must be made between ethnicity and nation, nationality can be formed by several ethnicities. It is essential that they have the will to unite. If a society has the ambition to build a nation and is deprived of the

support of power, it will not have its own identity, which is a characteristic not only of societies but also of states.

Among the direct manifestations of the identity of society are nationalism, active foreign policy, and for small and medium-sized countries the "besieged fortress" syndrome. This is especially characteristic of the countries of the Caucasus region and Ukraine – in the post-Soviet space, where the growth of national consciousness continues. Another example is the countries of the former Yugoslavia, where some of them still lack an element of national identity, but a manifestation of nationalism based on ethnic differences. Thus, as factors that indicate a readiness to create a single nation, national self-awareness and a sense of identity stand out, which on the one hand seems divided (for example, ethnic and national), and on the other - united. Trends related to identity strengthening and weakening are manageable. As an example, Ukraine, Russia, by annexing Crimea and conducting a military operation, under the pretext of protecting the Russian population, contributes to the mobilization of a radical, maximum nationalist element on the territory of the country.

The free movement of the population and the openness of borders contribute to the weakening of state "unity". A person who understands the world turns from a tied "pawn" into a "citizen of the world", which is used by individual funds representing grants and internships abroad to "educate" emissaries with their ideology. However, according to Newton's third law, "action always has an equal and opposite reaction", and in the East this rule takes the form of a counter-trend, within which the traditional consciousness struggles with the introduction of foreign elements. Thus, the element of clan relations – tribalism – still prevails in the system of social interaction for the Maghreb countries. Moreover, pressure from the world community on a particular, marginal in their opinion, element of the system leads to a sharp reaction, but never to obedience. Iran's nuclear ambitions during the period of sanctions, the imprisoned militarized North Korean regime, the repressive regimes in the countries of the Horn of Africa are developing due to the popular consolidation around the nation's leader, as well as with the help of those who are dissatisfied with the conditional 'consensus'.

These countries are forced to develop their own military potential, to make contacts with individual formations as emissaries of their activities and thus undermine regional and global security.

### **2.6. The role of the "fourth" power**

Recently, information has become a key weapon of war. Even the small use of cyberspace provides great opportunities in terms of forming a space for the realization of the national interests of states, placing the "right" emphasis on the key events of modern history. Channels such as YouTube, Telegram, platforms such as "X", Facebook, LinkedIn are increasingly used, both to explain the development of the situation in areas of tension and to carry out propaganda aimed at one or the other of the warring parties. Last but not least, the "strong and rich" media broadcast live footage from the hot spots of the conflict, which once again changed public attitudes.

The phenomenon of social networks and ambassadors who repeatedly accelerate communication processes is increasingly the subject of discussion in political processes. The skillful use of informal methods to convey their point of view to the voter allows candidates in key countries around the world to win the presidential election (the role of the Facebook platform in the election campaign of D. Trump and the Telegram ambassador in Iran's 2017 presidential election), opposition groups to take people to rallies and stage revolutions (the influence of social networks on the intensity of protests during the 'Arab Spring') [3]. This is why one of the most politicized topics of public life today has become the problem of state control over information flows. Under these conditions, the thesis that myths and reality were in close proximity thanks to the activity of the media and communications, the resource of which is used by individual lobby groups, political parties, commercial corporations and entire countries [4]. A more pressing issue is the option of presenting the news from the 'strong and rich' media: a cleverly selected video sequence of the development of the conflict is the most effective means in terms of its impact. Considering the strengthening of the clip-awareness of young people who are unable to perceive information in long logically verified formats (articles, journalistic investigations, documentaries). Due to small information forms, idealized or hyperbolized negative image of state leaders, stable patterns of perception of states and societies are formed, which allows the elite, which increasingly focuses not on national, but on its own interests, to carry out the necessary actions. Such videos should be short and consistent, containing one ideology at a time (a classic example is the chain: "Assad is a dictator. Down with Assad! ", " Putin is a murderer! To arrest Putney! ", " Trump is a criminal! To deprive him of the right to participate in elections! " In the United States the tournament was broadcast live on CBS, ESPN, and Tennis Channel. Up to the minute, a well-chosen moment (for example, immediately after the end of Friday prayer in Muslim countries) is able to provide a difference from thousands of people who have come to the demonstrations, thus deciding the fate of the issue on the agenda in one direction or another. This toolkit is used today not only by the forces that opposed the current regimes. The state, when communicating with society, has also learned to transmit the necessary ideas through new methods of communication.

## **III. RESULTS AND DISCUSSION**

### **3.1. Promoting the role of the UN**

In order to increase the role of the UN internationally, steps can be taken to reform the organization at two levels, whereby at the regional (lower) level the organization can rely on individual regional structures, including political-economic and military, both at continental and intercontinental level, and at a more local level.

It is believed that at the territorial level, these organizations can act under the auspices of the UN, turning for assistance to other regional and intercontinental unions if necessary. This could allow the mechanism for implementing decisions to become more dynamic, strengthen ties between the world

organization and regional and mutually strengthen the authority of both the UN and regional organizations.

### **3.2. Increasing the role of "intermediary states" by using their influence in individual political and economic unions**

The struggle for supremacy and leadership in the world order is expanding the poles of the global international system. Nevertheless, the main "players", the US and Russia, are competing to increase and impose control over both energy and natural resources, as well as individual countries. This gives the new "players" a chance to act as a mediator in the settlement of regional conflicts – in particular Russia-Ukraine and Israel-Hamas, respectively Palestine.

Recent crises, the coronavirus pandemic and the war in Ukraine, Europe's energy dependence on Russia, have caused disagreements among EU leaders, which in turn sharply reduced the Union's influence in the global international system.

At this stage, achieving a fully neutral position on the part of China, India, the UAE, Saudi Arabia, South Africa, and Türkiye is difficult due to economic and energy dependencies on the one hand and on the other the opposition of the United States as a global leader to date.

Türkiye, through President Erdogan, is pursuing a controversial foreign policy mostly for economic gain. This leads to the withdrawal of trust in the country and the limitation of its influence.

### **3.3. Challenges to diplomacy**

Against the background of the changing international situation and the deepening regional conflicts (the Russian-Ukrainian, Middle East and Red Sea) and the risks of the emergence of new ones (Bosnia and Herzegovina, Kosovo, the Caucasus, North and South Korea, Iran, China and Taiwan, etc.) require the use of new methods of diplomacy. Thus, the terms innovative and mediation diplomacy are becoming more widely used among diplomatic communities. .7

Under an innovative approach, on the one hand, the use of the development of information technologies and social networks for indirect and non-verbal influence should be perceived to form public opinions and attitudes.

Leaders of individual countries, their representatives and official institutions are increasingly using social networks to send messages. Their goal is to generate broad public support and lead to concrete negotiations.

On the other hand, innovative diplomacy also means entrepreneurial and effective diplomacy, i.e. using innovative approaches to solve global and regional problems.

An important issue for enhancing the ability of persons involved in shaping foreign policy in the implementation of effective diplomacy is the provision of a reliable mechanism for collecting and evaluating information.

To innovative diplomacy can be added a search for wider supporters, representatives from different countries and communities and expressing a common view on the particular case or conflict, to be attracted as participants in the mediation process of negotiations between the warring parties.

An example of success in this regard could be Türkiye's efforts to mediate in resolving the Nagorno-Karabakh conflict between Azerbaijan and Armenia when Russia is sought to influence Armenia and Saudi Arabia and the UAE to influence Iran to end pressure on Azerbaijan.

It can be determined that an integral part of innovative diplomacy is mediation diplomacy, i.e. to use the abilities of persuasion to achieve understanding between the warring parties.

If in the past this was not applied because of the conquering ambitions, nowadays, by including "like-minded" people in the process, persuasion becomes more and more realistic. Of course, the attraction of additional participants is also based on mutual benefit on the one hand and the benefits that these countries will have on the other.

## **CONCLUSIONS**

The increased political activity of individual social and class actors (primarily in the virtual space) catalyzes group responsibility for the future of the nation, while reducing the frequency of charismatic leaders appearing in the political arena who would be willing to take responsibility not only for cosmetic changes, but also for structural reforms. The crisis of leadership can be extrapolated to the international plan, where there are more and more zones of instability, the dynamics of which are becoming increasingly destructive in the context of the lack of political will to initiate measures from the crisis management course. Exceptions to this list are China and Iran, as well as Russia and Türkiye. Leadership implies defining the goals and logic of the country's development, as well as the ability to gradually implement them in the form of a national domestic and foreign policy course. In this context, in order to enhance the role of the EU, it is necessary to undertake changes in the decision-making process and the establishment of a new leadership policy. At this stage, Türkiye's governance policy can be described as authoritarian and leadership change is needed to enhance its role as a mediator and mediator in the global international system. Given Erdogan's ambitions to "root" in the country, such a change will take time.

The emphasis on state development cannot take place outside the context of global disruption (agenda fluctuations between conservatism and liberalism). At this historical stage, the world has entered an era of rebellion of conservatism against liberalism; this process is observed in almost all key states of our time. Serious changes of this scale cannot occur without "surface fluctuations": changes in elites accompany crises, transformations in the field of indoctrinal policy design



provoke revision of previously unshakable paradigms. At the same time, the conflict plains are rarely preserved, the static of confrontation is not typical – both for forms, methods and for location. In this regard, clashes in the 'Greater Middle East' due to the discursive constraints of the participants will spread to the regions of Southeast Asia (the emergence of ISIL 'branches' in Indonesia, Malaysia and the Philippines) and the post-Soviet space (given the number of foreign fighters in Syria and Iraq, the South Caucasus and Central Asia are threatened), where many external elements are active. The key challenge within modern international relations can be called the need to find new rules of the game that reflect objective reality, but not speculative constructs that some actors ignore openly, others – non-public. In this sense, the discussion around the mutual legitimation of double standards is particularly valuable. The formation of a new foundation and alternative methods of diplomacy requires ideas for development and a global outlook based on an understanding of regional political technology processes and instruments.

#### REFERENCES

- [1] Charter of the United Nations (apis.bg)
- [2] Bogdanov, Plamen. Concepts, doctrines and strategies for security and armed struggle in the late XX and early XXI century. Treatise Sofia, 2023. 394 p. ISBN:978-619-185-589-6
- [3] <https://www.dw.com/bg/noviat-briks-vklucva-46-ot-svetovnoto-naselenie/a-66628211>), (statement by Brazilian President Luiz Inacio Lula da Silva)
- [4] Teodosiev P. Turkey's migration prevention policy. Interaction with the Bulgarian diplomatic and consular missions. – In: Proceedings of a Seminar on "Migratory Risk to the Republic of Bulgaria". – Sofia: Academic Publishing House of the Academy of the Ministry of Interior, 2023, pp. 231– 243, ISBN 978-954-348-243-6.
- [5] The American tradition of media bias//The Washington Times//url: <http://www.washingtontimes.com/news/2016/oct/18/americas-tradition-of-media-bias/>
- [6] Al Jazeera faces pressure to close amid Qatar's diplomatic crisis//NPR//url:<http://www.npr.org/2017/07/04/535530437/al-jazeera-faces-pressure-to-close-amid-qatars-diplomaticcrisis>.
- [7] Teodosiev, Plamen. Innovative and mediation diplomacy as a means of settling conflicts. Study 48 pp. ISBN 978-619-185-630-5. [Electronic resource] ISBN: 978-619-185-631-2.

# *Mission Command and the challenges of the Early 21-st Century*

**Nikolay Tsvyatkov,**  
NMU HQ Operation department  
Vasil Levski National military university  
Veliko Tarnovo, Bulgaria  
e-mail: lz2nzf@gmail.com

**Abstract.** Mission command as a phenomenon, mission command philosophy and challenges of the Early 21-st Century. This paper presents the results of the authors' research related to mission command and its role in planning and conducting operations in the early 21st century.

**Keywords:** *command and control, commander, leaders, mission command.*

## I. INTRODUCTION

In the chaos and uncertainty of modern war, our troops must be empowered to make decisions, take the initiative, and lead boldly. This is Mission Command: a command culture, leadership style, and operating concept that has been embraced by armed forces the world over. Real-world examples supported by in-depth research provide the who, what, when, where, and why of Mission Command, identifying opportunities to improve how we lead our teams. "Internationally, the contemporary security environment requires a continuous increase in the diversity of operations in which the Armed Forces are engaged" [1].

The 21st Century brings a vast selection of technology to support commanders and staffs, and increase the efficiency of formations; however, technology is not a substitute for leadership. Commanders cannot build organizational cohesion and mutual trust from a computer or demonstrate the attributes and competencies to influence confidence. Leaders must build success the old-fashioned way – in person. While mission command in the 21st century will have a lot of technology to support the commander, the principles have always been around; it requires skilled leadership to provide desired results [2].

The commander's intent is shared with subordinates, who are told what to achieve and why, but are then left to decide how to achieve it. Subordinates are encouraged to use their judgement, initiative, and intelligence in pursuit of the commander's goal.

Network-enabled capability could offer the opportunity to capitalize on the potential of new

technologies to decentralize tactical command whilst centralizing strategic command.

Thus, mission command could be enhanced by the full exploitation of the benefits of network-enabled capability, with shared situational awareness and shared understanding of commanders' intent. But it could also be undermined by it, both at the operational level and the grand strategic level of the political-military interface. There is a danger that mission command itself can encourage a preoccupation with goals (the commander's intent) rather than effects, which in the new operational environment could be undermined by the actions of those at the tactical level.

## II. MATERIALS AND METHODS

The materials used to develop the mission command theme are developed in detail in the references indicated. This report is my own analysis of mission command and its role in planning and conducting operations in the early 21-st century. The topic is truly relevant to the currently ongoing symmetrical combat operations. The stated thesis is the closest to my understanding of the essence of mission command and the challenges at the beginning of the 21-st century.

### **Higher command**

Most defense doctrine speaks of strategic, operational, and tactical levels of war, where instructions and objectives are passed down the chain of command from the top down, with each level given time to achieve certain objectives. But in high tempo full spectrum effects-based operations, tactical activity can often have strategic effects, many of which can occur without assessing what has been accomplished before it is too late. While strategic/tactical overlap may be unavoidable given the nature of some operations, it threatens the basic command and control structure and can undermine mission command principles. Pragmatism applied to prevailing military-political circumstances will be key, although political and military leaders at the strategic level should be discouraged from attempting to directly influence tactical activity. "We possess our own unique

*Print ISSN 1691-5402*

*Online ISSN 2256-070X*

<https://doi.org/10.17770/etr2024vol4.8209>

© 2024 Nikolay Tsvyatkov. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

combination of capabilities to: create, strengthen, innovate and unite” [3].

The challenge facing the units is that effects-based operations combined with network-enabled capability may not permit such pragmatism in the future because there simply may not be the time. Effects-based operations will not be linear or sequential and control of their environment will become more complex and difficult.

Additionally, the technology of network-enabling capabilities may encourage political leaders to believe that they have a better understanding of the battlespace than is actually the case. Civilian and even top level military control may become less, not more, effective. The results could be overwhelming and deeply confusing.

Mission command is a philosophy of leadership that focuses on the commander's intent and empowering subordinates to make decisions within that intent. The goal of mission command is to provide commanders with the flexibility to act and react quickly to changing situations while maintaining control over their unit.

The idea of Mission Command came out of studies done of the Napoleonic Wars. It's the model of leadership most taught to military forces but translates as a good model in any organization. If you look it up on Internet sites, they refer to it as “centralized intent with decentralized execution”.

Successful execution of mission command is possible if we demonstrate the “Seven Cs:” Character, Courage, Competence, Communication, Commitment, Compassion, and Confidence. All of these principles seem self-evident and none of them require explanation, but internalizing them, living them, and demonstrating them require vigilance and self-evaluation to enable mission command [4].

### **Mission command philosophy**

- People are the basis of all military organizations, and military operations occur as human interactions. Commanders use the philosophy of mission command to exploit and enhance uniquely human skills.

- Commanders implement mission command through the balancing of the art of command with the science of control.

- Exercise of authority and direction by the commander using mission orders to enable disciplined initiative within the **commander's intent** to empower agile and adaptive leaders in the conduct of unified land operations [5].

**Mission command** is the exercise of authority and direction by the commander using mission orders to enable disciplined initiative within the commander's intent to empower agile and adaptive leaders in the conduct of unified land operations [5].

A common view is a sine qua non for unity of effort among all those involved in operations. With the decentralized nature of command and control as a mission, without it there will be a lack of coordination and no coherence of action. If the commander's intent is not explicitly reflected in the common view, no command and control as a mission can exist. Every

mission includes two main parts - the task to be accomplished and the reason for it. The task refers to the actions to be taken, while the reason is related to the objective and the desired end state/desired outcome. While a possible change in the situation could make the task irrelevant, the goal is something enduring and permanent that motivates and guides actions and enables initiative to be shown despite disorder and change of environment.

The commander's intent (the objective) creates the conditions for cooperation of military structures in various /diverse/ operations, establishes the main purpose of the organization, more specifically on what to focus efforts. This in turn ensures maximum understanding / knowledge of the combat situation and provides the most important perspectives in the leadership of the organization. In a system based on command and control as the mission, ensuring the overall objective is the command's primary duty, its responsibility, and the most essential means of guiding the organization.

#### **An Army leader is [5]**

- Anyone who by virtue of assumed role or assigned responsibility inspires and influences people to accomplish organizational goals.

- Motivates people both inside and outside the chain of command to pursue actions.

- Anyone who emphasizes thinking and shape decisions for the greater good of the organization.

Model of Mission Command has five key priorities for leaders:

- **Selection and maintenance of the aim:** you must have a clear and compelling purpose. In your organization you might call it your vision. You need to know what your aim is and stick to it.

- **Building trust and mutual understanding:** you must make sure that you are communicating, training, empowering, and trusting. This makes sure that everybody knows the aim and knows the role they have in achieving that aim.

- **Aligning objectives:** everybody plays a little part in achieving the aim, each of those little parts must fit together to make the machine work. It's the role of leaders to have an overview of those objectives to make sure they align.

- **What and why, not how:** what and why sits with the leaders, the how sits with everybody else. You must give people the responsibility to work out their own How to make sure that they have ownership of delivering on their objective. Trust means ownership, which means accountability.

- **Tempo:** achieving aims and objectives required action and when we're done planning, we need to get on and activate our decisions. When there is a steady drumbeat of activity, momentum is generated, things get done and people feel a sense of achievement.

#### **Build cohesive teams through mutual trust [5]**

##### **➤ BUILD COHESIVE TEAMS**

- Effective commanders build cohesive teams in an environment of mutual trust.

- Show you trust your teammates by involving them.
- Requires effort to overcome differences.

#### ➤ **MUTUAL TRUST**

- shared confidence among commanders, subordinates, and partners.
- Few shortcuts to gaining the trust of others.
- Trust takes time and must be earned.
- Put **trust** in, and you will generally **get trust** in return.

The great challenge is for leaders to hold their nerve and allow their organizations to operate in a Mission Command way, to steer clear of the detail and let the experts get on and deliver their objectives.

Mission command is an approach to command and control that enables subordinates to make decisions and execute in a decentralized manner appropriate to the situation. Mission command supports the concept of land operations and its emphasis on seizing, retaining, and using the initiative. War is inherently chaotic and uncertain. No plan can account for all possibilities, and most plans must be changed rapidly during execution to account for changes in the situation. No one person is ever informed enough to make every important decision, nor can one person keep up with the number of decisions that must be made during combat operations. Subordinate leaders often have a better sense of what is going on during the battle and are more likely to respond effectively to threats and fleeting opportunities if they are allowed to make decisions and act on changing situations and contingencies not considered in the original plan to achieve their commander's intent.

Enemy forces may behave differently than expected, a route may become impassable, or units could consume supplies at unexpected rates. Friction and unforeseeable combinations of variables impose uncertainty in all operations and require an approach to command and control that does not attempt to impose perfect order, but rather accepts uncertainty and makes allowances for unpredictability.

ADP 6-0, Mission Command, discusses the fundamentals of mission command, command and control, and the command and control function of combat operations. It describes how commanders, assisted by their staffs, combine the art and science of command and control to understand situations, make decisions, direct actions, and lead forces toward mission accomplishment.

The use of the term "mission command" to describe multiple things-military function, system, and philosophy-created unintended ambiguity. Mission command replaced command and control, but in practical application often meant the same thing. This led to different expectations regarding the appropriate application of mission command during operations and other activities. Labeling multiple things as mission command inadvertently undermined the importance of mission command, which is critical to command and control of forces across the spectrum of military operations. Distinguishing mission command from command and control provides clarity, allows leaders to focus on mission command in the context of the missions

they execute, and aligns the understanding of their own units with those of multinational partners, all of whom use the term command and control. "The asymmetric nature of security threats and risks comes to the fore" [6].

#### **Command & Control Warfighting Function**

The command and control warfighting function are the related tasks and a system that enable commanders to synchronize and converge all elements of combat power. The primary purpose of the command and control warfighting function is to assist commanders in integrating the other elements of combat power to achieve objectives and accomplish missions. The command and control warfighting function consists of the command and control warfighting function tasks and the command and control system.

The command and control warfighting function tasks focus on integrating the activities of the other elements of combat power to accomplish missions. Commanders, assisted by their staffs, integrate numerous processes and activities within their headquarters and across the force through the mission command warfighting function:

- Command forces
- Control operations
- Drive the operations process
- Establish the command and control system [7].

### III. RESULTS AND DISCUSSION

#### **Understanding the seven mission command principles**

The main principle of mission command is that leaders lead and operational people operationalize. These leaders are the ones that micromanage and get too involved in the day-to-day tasks of the businesses, to the point that people ask, why don't they just do it themselves? By working to 'mission command' principles, you can bring the attention of leaders back on track and they focus on the why and the what, not the how.

Leadership is challenging, demanding, and burdensome but rewarding, stimulating, and accomplishing. Mission command is a critical element of successful leadership. The philosophy allows commanders to make quick decisions and take action to achieve their objectives. This blog post will define mission command and discuss how each principle can be applied in leadership.

#### **What is Mission Command? [8]**

According to the Department of the US Army, mission command is, "the Army's approach to command and control that empowers subordinate decision-making and decentralized execution appropriate to the situation."

Mission command is a philosophy of leadership that focuses on the commander's intent and empowering subordinates to make decisions within that intent. The goal of mission command is to provide commanders with the flexibility to act and react quickly to changing situations while maintaining control over their unit.

### **The 7 Principles of Mission Command [8]**

Mission command requires competent forces and an environment of mutual trust and shared understanding among commanders, staffs, and subordinates. It requires effective teams and a command climate in which subordinates are required to seize opportunities and counter threats within the commander's intent. Commanders issue mission orders that focus on the purpose of an operation and essential coordination measures rather than on the details of how to perform assigned tasks, giving subordinates the latitude to accomplish those tasks in a manner that best fits the situation. This minimizes the number of decisions a single commander makes and allows subordinates the greatest possible freedom of action to accomplish tasks.

Finally, when delegating authority to subordinates, commanders set the necessary conditions for success by allocating appropriate resources to subordinates based on assigned tasks.

Successful mission command is made possible by the seven principles of mission command that commanders must understand and apply to create a shared understanding within their unit and ultimately achieve success on the battlefield.

#### ***Competence***

Commanders must clearly understand what they are doing and be able to execute their tasks confidently. They must also be able to explain their decisions and actions to their subordinates. Tactically and technically competent commanders, subordinates, and teams are the basis of effective mission command. An organization's ability to operate using mission command relates directly to the competence of its Soldiers. Commanders and subordinates achieve the level of competence to perform assigned tasks to standard through training, education, assignment experience, and professional development.

Commanders continually assess the competence of their subordinates and their organizations. This assessment informs the degree of trust commanders have in their subordinates' ability to execute mission orders in a decentralized fashion at acceptable levels of risk.

#### ***Mutual Trust***

Commanders must trust their subordinates to make decisions and carry out tasks independently. They must also trust their subordinates to provide honest feedback. Mutual trust is essential to successful mission command, and it must flow throughout the chain of command. Subordinates are more willing to exercise initiative when they believe their commander trusts them. They will also be more willing to exercise initiative if they believe their commander will accept and support the outcome of their decisions. Likewise, commanders delegate greater authority to subordinates who have demonstrated tactical and technical competency and whose judgment they trust.

#### ***Shared Understanding***

A critical challenge for commanders, staffs, and unified action partners is creating shared understanding of an operational environment, an operation's purpose, problems, and approaches to solving problems. Shared understanding of the situation, along with the flow of information to the lowest possible level, forms the basis for unity of effort and subordinates' initiative. Commanders and staffs actively create shared

understanding throughout the operations process (planning, preparation, execution, and assessment). They collaboratively frame an operational environment and its problems, and then they visualize approaches to solving those problems.

#### ***Commander's Intent***

Commanders must clearly articulate their vision and intent for the mission. This will help subordinates make decisions and take action even when the commander is not present. The commander's intent becomes the basis on which staffs and subordinate leaders develop plans and orders. A well-crafted commander's intent conveys a clear image of an operation's purpose and desired end state. The commander's intent provides a focus for subordinates to coordinate their separate efforts.

#### ***Mission Command Orders***

Mission orders are directives that emphasize to subordinates the results to be attained, not how they are to achieve them. Mission orders enable subordinates to understand the situation, their commander's mission and intent, and their own tasks. Commanders must give subordinates clear and concise orders focused on the mission, not on how to accomplish the mission. This allows subordinates to use their own initiative and judgment to complete the task.

#### ***Disciplined Initiative***

Disciplined initiative refers to the duty individual subordinates have to exercise initiative within the constraints of the commander's intent to achieve the desired end state. Simply put, disciplined initiative is when subordinates have the discipline to follow their orders and adhere to the plan until they realize their orders and the plan are no longer suitable for the situation in which they find themselves. Subordinates must exercise disciplined initiative within the commander's intent. This means they must take action to accomplish the mission based on the commander's order.

#### ***Accepting Risk***

In general terms, risk is the exposure of someone, or something valued to danger, harm, or loss. Because risk is part of every operation, it cannot be avoided. Commanders analyze risk in collaboration with subordinates to help determine what level of risk exists and how to mitigate it. Commanders and subordinates must be willing to accept risk. This means they must be willing to take risks that may lead to failure and have the courage to seize opportunities that may lead to success. Reasonably estimating and intentionally accepting risk is not gambling. Gambling is making a decision in which the commander risks the force without a reasonable level of information about the outcome. "Since decision making is knowledge, then all organizations (systems) learn throughout their existence, and a learning security system generates and manages its own knowledge in the information age of knowledge under the ever-increasing need to systematize relationships (operationalize) within itself" [9].

### **CONCLUSIONS**

The mission command approach to command and control requires active participation by personnel of all ranks and duty positions.

Subordinate officers, noncommissioned officers, and soldiers all have important roles in the exercise of mission command.

During operations, subordinates are delegated authority, typically through orders and standard operating procedures, to make decisions within their commander's intent.

Commanders expect subordinates to exercise this authority to further the commander's intent when changes in the situation render orders irrelevant, or when communications are lost with higher echelon headquarters.

#### 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] <https://institute.nvu.bg/bg/statia/ceIi-na-upravlenieto-na-sistemata-za-voenna-sigurnost>
- [2] Jack T. Judy, Lieutenant Colonel (Ret.), U.S. Army, Chapter 1 in „Mission command in the 21st century: empowering to win in a complex world“/ general editors Nathan K. Finney and Jonathan P. Klug., Fort Leavenworth, Kansas: The Army Press, [2016], LCCN 2016001491|ISBN 9781940804248 (pbk.), iv.[Online] Available: <http://lccn.loc.gov/2016001491>
- [3] Marinov, Rumen, Styles of management for Military Security System, 2020, KSI Transactions on, Knowledge Society A publication of the Knowledge Society Institute, Volume XIII, Number 2, June 2020, ISSN 1313-4787, p. 24-27
- [4] Robert B. Brown, Lieutenant General, U.S. Army Commanding Combined Arms Center and Fort Leavenworth, "Foreword" in „Mission command in the 21st century: empowering to win in a complex world“/general editors Nathan K. Finney and Jonathan P. Klug., Fort Leavenworth, Kansas: The Army Press, [2016], LCCN 2016001491 | ISBN 9781940804248(pbk.),iv. [Online] Available: <http://lccn.loc.gov/2016001491>
- [5] Virginia National Guard, "Mission-Command-And-Leadership-Development"[Online].Available: <https://va.ng.mil/Portals/55/Documents/Foxhole/Mission-Command-And-Leadership-evelopment.pptx?ver=eofMK-EIOfeEI-9R-KiD0A%3D%3D> [Accessed: Jan. 30, 2024].
- [6] Marinov, Rumen, Stoykov, Stoyko, Marinov, Petar, Urbanized territories non-existing part of crisis response operations, International Conference on Creative Business for Smart and Sustainable Growth, CreBUS 2019; Sandanski; Bulgaria; 18 March 2019 through 21 March 2019; Category numberCFP19U17-ART; Code 152084, ISBN: 978-172813467-3, Source Type: Conference Proceeding, Original language: English, DOI: 10.1109/CREBUS.2019.8840084, Document Type: Conference Paper, Publisher: Institute of Electrical and Electronics Engineers Inc.
- [7] Army Publishing Directorate, "ADP 3-0" [Online].Available:[https://armypubs.army.mil/epubs/DR\\_pubs/DR\\_a/ARN18010-ADP\\_3-0-000-WEB-2.pdf](https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18010-ADP_3-0-000-WEB-2.pdf) [Accessed: Jan. 31, 2024].
- [8] Army Publishing Directorate, "ADP 6-0" [Online].Available:[https://armypubs.army.mil/epubs/DR\\_pubs/DR\\_a/ARN34403-ADP\\_6-0-000-WEB-3.pdf](https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN34403-ADP_6-0-000-WEB-3.pdf) [Accessed: Jan. 31, 2024].
- [9] Marinov, Rumen, Dynamics in the theory and practice of the strategic management, 2018 International conference on High Technology for Sustainable Development HiTECH 2018, June 2018, Sofia, Bulgaria, ISBN: 978-1-5386-7039-2, Date Added to IEEE Xplore: 10 December 2018, ISBN Information: INSPEC Accession Number: 18308427, DOI: 10.1109/HiTech.2018.8566527, Publisher: IEEE, Conference Location: Sofia, Bulgaria, pp 11-14

# *Command and Control System of the Country's Defense*

**Nikolay Tenev Urumov**  
*Vasil Levski National Military University*  
Veliko Tarnovo, Bulgaria  
nturumov@nvu.bg

**Abstract.** The article reveals the nature and content of the Defence of the country and compares the nature of the leadership, command, and control concepts. It also reveals the purpose and content of the leadership, command, and control system. Based on this research, the author offers a definition of the leadership, command, and control system of the country's defence.

**Keywords:** *Command; Control; Leadership; Leadership, command, and control system of country's defence.*

## I. INTRODUCTION

The strategic security environment in the long term will be mainly characterized by increasing dynamics, acceleration and complication of destabilizing processes, and increasingly difficult identification of the origin and scope of threats and risks. Globalization will continue to be the main factor influencing geopolitical trends.

The boundaries between external and internal security are increasingly blurred. The combined use of classic and hybrid means to achieve the intended goals is becoming increasingly intense, and these factors will make the sources of threats difficult to identify, and respectively will make it difficult to prevent and deal with them. Hybrid threats will have an increasingly negative impact on national and collective security, and in this context, the boundary between the state of classically known war and peace will blur. The military tool alone is insufficient to address hybrid threats [1].

To optimally use the available resources and effectively deal with the challenges of the security environment, the Republic of Bulgaria implements a security policy based on preventive and proactive approaches and solutions, coordinated and complementary efforts involving the political, military, economic, civil and the information resources of the country.

Although our country considers its security as an integral part of allied security and relies on collective efforts to successfully counter modern risks and threats,

the main goal of our security policy is the creation and maintenance of national power to ensure the security of the country. We can argue that in contemporary security environment, the role of non-military components as part of the national power to guarantee the security of citizens, territorial integrity and sovereignty of the country is significantly increasing. At the same time, the role of the military component, created and maintained to neutralize military threats and ensure military security, is preserved, as evidenced by the war in Ukraine and the conflict in the Middle East. Therefore, we can claim that the main goal of the security policy is achieved by actively creating a favourable international environment, which excludes the occurrence of a military crisis against the country, and in the event of such a crisis, provides sufficient potential, allowing adequate reflection of aggression, and if necessary, creating conditions for conducting allied operations to guarantee the sovereignty and territorial integrity of the country.

The above mentioned is confirmed by what is written in the National Defence Strategy that "The country's defence is planned, prepared and implemented within the framework of NATO's collective defence and the Common security and defence policy of the EU with effective use of national armed forces." [2].

To successfully implement the country's defence tasks in the indicated manner, it is necessary to build and maintain a sufficiently ready system for leadership, command, and control. An analysis of the available literature on these issues shows that some of the existing regulations no longer fully meet the challenges of the contemporary security environment. Therefore, it is necessary to take appropriate action to overcome the existing deficits.

To be able to take such actions, it is imperative that we fully understand the nature, purpose and content of the leadership, command, and control system of the country's defence. Therefore, the purpose of the present study is to analyse and reveal its nature, purpose, and content and

*Print ISSN 1691-5402  
Online ISSN 2256-070X*

<https://doi.org/10.17770/etr2024vol4.8215>

© 2024 Nikolay Tenev Urumov. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

based on this to propose a new definition of the system, to adequately address the issue and actualise the existing regulatory framework.

## II. MATERIALS AND METHODS

To achieve this goal, the nature and content of the country's defense is revealed. A comparative analysis of the essence of the concepts of leadership, command and control is done, as well as a functional analysis of the purpose and content of the system for leadership, command and control of the country's defense.

## III. RESULTS AND DISCUSSION

### A. *Nature and content of the country's defence*

The nature and content of the country's defence are discussed in the main conceptual and program documents for national security. They are regulated in the Law on Defence and the Armed Forces of the Republic of Bulgaria and in the resulting by-laws. According to the Law on Defence and the Armed Forces, "The defence of the Republic of Bulgaria is a system of political, economic, military, social and other activities to ensure a stable security environment and to prepare and implement armed protection of the territorial integrity and independence of the state. It is part of national security, which is determined by national interests." [3].

The above mentioned gives us reason to claim that the defense of the country is part of the national security system and is, in its nature, a system of military and non-military activities of state bodies and institutions, the armed forces, non-military organizations and citizens aimed at strengthening international peace and security, creating conditions for preventing a military threat against our country, building, maintaining and, if necessary, using defense capabilities to prevent and counter crises of a military nature, threatening our national security.

According to the article 6 of the Law on Defence and the Armed Forces "Defense of the country ensures: creation, maintenance and use of the country's necessary resources for the formation and maintenance of a stable security environment; protection of the territory and the population in case of military threats and in wartime; creation, maintenance and management of the national resources and means of defense of the country outside the resources and means of the strategic plans and the plans of operations of the armed forces.

The above mentioned activities are carried out through:

- joint action with NATO allies, European Union member states and international organizations to create a stable security environment.
- forecasting military threats and defence planning.
- preparation and maintenance the armed forces of the Republic of Bulgaria in the necessary combat, operational and mobilization readiness, as well as the ability to deploy.
- preparation of the country's infrastructure for defence.

- conducting surveillance and intelligence.
- logistic support and maintenance of the armed forces.
- protection of the state border.
- preparing the population and the economy of the country for action in the event of military threats and/ or in wartime.
- preparation and maintenance of the armed forces to be use in disasters relief.
- development of an integrated communication and information system.
- maintaining cooperation with allied and other countries, international governmental and non-governmental organizations.
- military-patriotic training and education of the population of the country.
- conducting defence and mobilization training." [3].

The above mentioned activities actually determine the content of the defense of the country. Analysing these provisions of the Law on Defence and the Armed Forces we can argue that leadership, command, and control system is a crucial part of the country's defense. Therefore, in order to be able to explore this system we should well know nature and content of the country's defense.

### B. *The nature of the leadership, command, and control concepts.*

Leadership is an activity based on the existing legislation in the country, which covers the activities of managing the entire resource of an organization and especially its human resources. According to the Doctrine of the Armed Forces of Bulgaria, "leadership is a process that encompasses all personnel and includes a leader and subordinates. The purpose of this process is to make decisions, give tasks, organize, and control their implementation to achieve defined goals. The leader is a person who occupies the highest position in the hierarchy of the organizational structure and carries out leadership. The leadership is the activity and responsibility of the political and military-political leadership of the country." [4].

Taking these statements into account, we can assume that leadership is carried out by political leaders, and supreme military commander and the main task of this activity consists in defining political goals and providing the necessary resources to achieve the goals.

Command is an activity carried out within the armed forces and "includes the processes by which the commander makes a decision, imposes his will and communicates his intent to his subordinates. Command at all levels is the art of decision-making, motivating and directing the actions of subordinates to accomplish assigned missions and tasks. This requires a clear vision for achieving the desired results and a common understanding of the concept, mission and priorities, as



well as the ability to adequately allocate resources, manage subordinates and risks, and assess the situation.” [4].

Subjects of command are the persons who have rights, obligations, and responsibilities to direct the activities of their subordinate formations. Holders of such attributes of power are commanders, and superiors, who are at the top of the hierarchical pyramid of organizational units of the armed forces.

A comparative analysis of the concepts of leadership and command shows that both imply powers given to an individual to exercise his will over subordinates and structures, with the difference that the leader is usually a civilian (political) person who leads military and non-military persons and structures, and the commander is a serviceman who commands servicemen and military structures. At the strategic level, leaders can also lead and manage military structures, if this is regulated by law.

According to the Doctrine of the Armed Forces of the Republic of Bulgaria, “Control is the power exercised by the respective commander over the activities of his subordinate structures or other structures that are not usually under his command. This power includes responsibility for the execution of orders or directives. All or part of the power may be transferred or delegated. Control allows the commander to monitor the actions and their effectiveness in realizing the intent of the senior commander and achieving the objectives of the operation. Command and control are interrelated and relate to the activities of the commander and staff. There can be no sign of equality between them. Control is just an aspect of command.” [4].

The analysis of these statement allows us to conclude that control is a purposeful activity through which the leader (commander), assisted by his working body (headquarters), organizes, coordinates, and controls the activities of his subordinates in performing their assigned missions and tasks. Control as a process includes continuous collection, study, analysis, and evaluation of information; decision making; assignment of tasks to subordinates; operations and actions planning; organizing interaction and coordination; organizing a control system; organizing and conducting constant effective control for the implementation of the assigned tasks and achieving the set results.

The significant similarity in content and functionality between the leadership and the command gives grounds to argue that when considering the control processes in non-military structures we can assume that a special system is built in them, called leadership and control system, like the command and control system in the Armed Forces.

To better understand the essence of the system of leadership, command, and control of the country’s defence, in addition to issues related to the nature of the concepts of leadership, command and control, it is necessary to analyse the purpose of this system.

#### *C. Purpose of the system for leadership, command, and control of the country’s defence*

According to the Doctrine of the Armed Forces, “the main goal of the command and control system is to

maintain command through forming a common operational picture; supporting decision-making by reducing time and improving accuracy; preparation and dissemination of directives (orders).” [5].

The analysis of these statements, as well as above mentioned for the nature of leadership, command and control concepts give reason to conclude that in the Doctrine of the Armed Forces the purpose of the system of leadership, command and control is incomplete.

Bearing in mind the considerations made above about the nature of leadership, command and control, it can be argued that, apart from the formation of a common operational picture, support for decision-making and the preparation and dissemination of directives, the purpose of the leadership, command and control system must also address issues related to collecting and analysing information, determining goals and desired results, defining tasks and their distribution among available capabilities, as well as in time and space, and last but not least, performing control of the tasks implementation and desired results achievement.

Therefore, the main purpose of the of leadership, command and control system of the country’s defence should include the following:

- continuous collection and analysis of information for assessment of the military-strategic environment and formation of a common operational picture.
- based on the assessment formulating goals and defining tasks for their achievement.
- decision making how to assign the tasks, both among the available capabilities and in space and time, to achieve the defined goals.
- preparation and dissemination of directives, orders, guidance, and instructions.
- providing feedback and control for the implementation of the tasks and achieving the desired results.

Knowing the nature of the leadership, command, and control concepts as well as the purpose of the leadership, command, and control system, to understand fully this system it is essential its content to be revealed.

#### *D. Content of the system for leadership, command, and control of the country’s defence*

According to the Doctrine of the Armed Forces the content of leadership, command and control system “includes:

- the personnel performing the planning and management processes, as well as the personnel ensuring activities of the former.
- infrastructure and equipment (command posts with the relevant equipment for the work and life of the personnel) and an integrated Communication and information system (CIS).

- Procedures - Standard Operating Procedures (SOPs)" [6].

Careful reading of the main regulatory documents shows that the personnel carrying out the processes of leadership, command and control include the country's top political leadership, including the President, the Council of Ministers, and the Minister of Defence, as well as commanders, and superiors at all levels of the Armed Forces, including the Chief of Defence, the commanders of the Joint Forces Command and services, the commanders of the formations of the Bulgarian Army and the commanders and superiors of the structures directly subordinated to the Minister of Defence.

Infrastructure and equipment usually include command posts with the appropriate equipment for work and life of personnel and an integrated CIS.

The command posts are specially equipped and provide places from which the leadership, command and control of the armed forces is carried out when bringing them to higher states and levels of combat readiness, preparation, planning and conduct of operations. These are the places where the flow of information about the situation is concentrated, the data is processed, the information is analysed, the situation is assessed, the decision is made, the tasks are assigned, the implementation of the tasks and the achievement of desired results is controlled.

An integrated CIS for the management of the country and the armed forces in a state of emergency, or state of war is a single, integrated organizational and technical complex of forces, equipment, and software to provide commanders and staffs, at any time and place, accurate, timely and protected information flow, ensuring effective and precise management and interaction between troops.

According to Allied Administrative Publication-6 NATO Glossary of Terms and Definitions (AAP-6) "the SOPs is a set of instructions applicable to those features of operations that lend themselves to a definite or standardized procedure without loss of effectiveness." [7].

The SOP may be presented as a sequence of actions or operations that must be performed in the same way to obtain the same result, under the same circumstances. Each system needs certain and effective procedures to function properly. SOP represent an algorithm for the functioning of the elements of the system as a single organism. They help create synergies and acquire new qualities of the system.

Each complex system, created by many subsystems, quite naturally is characterised by tendency for chaos and disintegration under the influence of various internal and external factors and the striving of individual subsystems to gain independence. To preserve the integrity and prevent the breakdown of the complex system, rules for the functioning and interaction of the individual

subsystems must be introduced. One of the ways to introduce such rules is the SOPs.

#### CONCLUSION

Bearing in mind all the considerations made above we can conclude that the establishment and development of the leadership, command, and control system of the country's defence in peacetime, in crisis and in wartime is essential for the effective functioning of the national security and defence system.

All of the above presented analyses about nature, purpose and content of the leadership, command and control system of the country's defence allow us to arguably propose a new definition – *Leadership, command and control system of country's defence is a complex of interconnected subsystems, including leaders and commanders, command posts, communication and information system and rules for functioning, which is built in peacetime at the political, strategic, operational and tactical levels and maintains readiness for leadership, command and control of the defence, the armed forces and the non-military components in peacetime, in crises and in wartime.*

The analysis of the purpose of the leadership, command and control system shows that a review of the regulatory documents is necessary, and in addition to the issues reflected now, the issues related to the collection and analysis of information, the determination of goals and tasks, and control or their execution should be addressed.

Issues related to the nature, purpose and content of the leadership, command and control system of the country's defence considered and analysed in this study do not fully exhaust the content of the topic. Nevertheless, the proposed material provides opportunity to study it and could be a good basis for discussions and debates to further improve it.

#### REFERENCES

- [1] Programme for Development of Defence Capabilities of the Armed Forces of the Republic of Bulgaria 2032. Sofia, State Newspaper, 2021, p. 6.
- [2] Defence Strategy of the Republic of Bulgaria. Sofia, MoD, 2016, p. 10.
- [3] The Law of the Defence and the Armed Forces of the Republic of Bulgaria. Online, <https://www.lex.bg> [Accessed February 26, 2024].
- [4] Doctrine of the Armed Forces of the Republic of Bulgaria. Sofia, MoD, 2017, p. 37.
- [5] Doctrine of the Armed Forces of the Republic of Bulgaria, Sofia, MoD, 2017, p. 38.
- [6] Doctrine of the Armed Forces of the Republic of Bulgaria, Sofia, MoD, 2017, p. 39.
- [7] NATO Glossary of Terms and Definitions, AAP-6. Brussel, NATO Standardization Office, 2020, p. 122.

# *Improving the Leadership, Command and Control System of the Country's Defense*

**Nikolay Tenev Urumov**

*Vice Rector for Education and Science  
Vasil Levski National Military University  
Veliko Tarnovo, Bulgaria  
nturumov@nvu.bg*

**Abstract.** The article analyses the current state of the country's defence leadership, command, and control system. Based on this research, three possible directions for its optimization have been formulated. The author argues the thesis that increasing the effectiveness of the system for leadership, command, and control of the country's defence is possible through improvement of the legal framework, organizational improvement of the system and technological modernization.

**Keywords:** *leadership, command, and control system; defence of the country.*

## I. INTRODUCTION

Following the accession of the Republic of Bulgaria in NATO and the EU, "the country's defence is planned, prepared and implemented within the framework of NATO's collective defence and the Common security and defence policy of the EU with effective use of national armed forces." [1] Having this in mind and trying to respond to the challenges of a rapidly changing and unpredictable security environment in the best way possible, Bulgaria changed its approach for development of defence capabilities from a threat-based to a capabilities-based approach.

The Armed Forces of the Republic of Bulgaria as a significant part of defence capabilities are in a process of dynamic transformation. "The development of troops and forces must ensure the maintenance of effective, combat-ready, multifunctional, modular and mobile military units with capabilities for joint action, for deployment in the country or abroad, relatively independent and adequately supplied." [2] They must be able to respond to current security environment challenges in a timely manner and be interoperable with Allied forces. In order to meet these requirements and effectively and efficiently implement the tasks set by the state leadership, it is necessary a clearly understandable and fully operational leadership,

command, and control system of the country's defence to be established and kept in required readiness state.

The analysis of the available doctrinal documents and the existing theoretical and scientific works on these issues shows that some of the statements in them no longer fully reflect the challenges of the security environment and do not sufficiently represent the modern views on the defence of the country in the system of collective security.

Therefore, the aim of this paper is to reveal some existing problems in the leadership, command and control system of the country's defence in peacetime, crisis and wartime, through a study of its theory and practice, and on this basis to propose guidelines for its improvement.

## II. MATERIALS AND METHODS

The system analysis method was used to assess the current state of the leadership, command, and control system, while the organizational interrelationships between the individual elements of the system and their functions and tasks were evaluated.

## III. RESULTS AND DISCUSSION

The research done below shows that the improvement of the country's defence leadership, command and control system can be done in three directions – regulatory framework, organizational and technological.

### *A. Improvement of the regulatory framework*

The development of an adequate regulatory framework is possible through a thorough analysis of the current state of the leadership, command, and control system, as well as the factors influencing its functioning. This will allow clarification of the rights and responsibilities of the management bodies and the functional relationships between them and identify measures to improve the organizational structure, develop

*Print ISSN 1691-5402*

*Online ISSN 2256-070X*

<https://doi.org/10.17770/etr2024vol4.8216>

© 2024 Nikolay Tenev Urumov. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

adequate work procedures and determine the requirements for personnel training.

The changes in the security environment that occurred after the end of the cold war, the emerging new risks, and threats, as well as the existing imbalance between the planned defense capabilities and the resources available for their development necessitated several strategic defense reviews to be conducted from the beginning of the new century until now. The last one was held in 2019-2020.

Based on the reviews, a number of amendments and additions were made to the Law on Defense and the Armed Forces of the Republic of Bulgaria. National Security Strategy, National Defense Strategy and Armed Forces Doctrine were developed and subsequently updated. The specified documents create the necessary legal framework, regulating the structure and functioning of the system for leadership, command, and control of the country's defense at the strategic, operational, and tactical level in a way that ensures management efficiency and achievement of the set goals.

However, despite the above, the analysis of the regulatory framework necessitates the conclusion that, along with the achieved results, there are also some shortcomings. First, the existing regulations define in the necessary details the system of command and control in the armed forces. However, this is not the case for the political leadership of the defense. For example, the functions, responsibilities, procedures, and mechanisms for functioning of the Supreme Command are not regulated in sufficient detail. Next, the responsibilities and the interaction of the state institutions to ensure the interaction of the military and non-military components of the country's defense system are not fully clarified. Also, the existence of a special leading or coordinating body to deal with the problems of the country's defense in peacetime is not regulated. The question regarding the interaction of the system for leadership, command, and control of the country's defense with the NATO Command Structure has not been clarified in detail, as well.

These shortcomings allow us to conclude that to achieve higher efficiency and effectiveness in the functioning of the leadership, command, and control system of the country's defence it is necessary:

a) The National Defence Strategy should define the leadership, command, and control system of the country's defence, distinguishing the political, strategic, operational, and tactical levels and defining the bodies for leadership, command and control, in peacetime, in crises and in war.

b) The Law on Defence and the Armed Forces of the Republic of Bulgaria should be repealed, and the Law on the Armed Forces of the Republic of Bulgaria and the Law on Defence of the Country should be adopted. The Law on the Defence of the Country should regulate the responsibilities, powers and obligations of the leadership, command, and control system of the country's defence, and must:

- regulate in more detail the functions, procedures, and mechanisms for the functioning of the Supreme Command.

- formulates the responsibilities and interaction of state institutions for the management of the military and non-military components of the country's defense system in a way that ensures the interaction between them.
- clarify the responsibilities, procedures, and mechanisms for the operation of the country's defense leadership, command and control system in a way that allows effective interaction with the NATO command structure, when accepting alliance assistance to guarantee the country's independence, sovereignty, and territorial integrity.

c) To be adopted a new Crisis Management Act, which:

- defines the functions of the central and regional bodies of the executive power and clearly allocates responsibilities among state institutions in crisis management.
- clarifies the place and responsibilities of the country's defense leadership, command and control system within the national crisis management system.

d) The formation of a specific permanent national body for peacetime management of the country's defence to be regulated, which will ensure the implementation of the tasks of preparing the country for smooth transition from peacetime to crisis and to state of war and normal functioning of the leadership, command, and control system of the country's defence in such cases.

e) An update of Doctrine of the Armed Forces of the Republic of Bulgaria is required, which:

- regulates the responsibilities, procedures, and mechanisms for functioning of the Armed forces Command and Control System and the procedure for its interaction with the governing bodies of the non-military components of the country's defence system.
- clarifies the responsibilities, procedures, and mechanisms for the functioning of the Armed forces Command and Control system and its interaction with the NATO Command Structure when accepting allied assistance to ensure the independence, sovereignty, and territorial integrity of the country.

#### B. Organizational structure improvement

The systematic approach allows the leadership, command, and control system of the country's defence to be considered as a complex hierarchical system consisting of subsystems, components, and elements, structurally united by interconnections between them, with certain potential to achieve a common goal and desired end state in defined conditions.

Applying a systemic approach to the analysis of the country's defense leadership, command and control system shows that it has a hierarchical structure, as its constituent parts are built on three levels - strategic, operational, and tactical. At each of these levels, functional subsystems are built with a unified structure

within certain limits, but with a different composition, state, and mode of operation. The analysis shows that, in general, the system is suitable to respond to current challenges, but there are also some shortcomings. For example, there are some difficulties if individual elements of the system need to operate decentralized and autonomously. It can also be said that there are certain difficulties when the system or its individual elements are faced with hybrid threats and constant attempts for deception and disinformation.

The main directions for achieving greater flexibility, mobility and sustainability of the command, command and control system, and for increasing its capabilities for decentralized functioning and implementation of the processes of information collection, processing and exchange can be systematized as follows:

- To build and maintain capabilities for rapid short-term formation of mission or target-oriented commands. This stems from the need for individual elements of the armed forces to be used to solve a wide range of tasks in peacetime, crises, and war. Furthermore, given our membership in NATO, the existence of such governing bodies will allow for more effective integration of formations from national armed forces into Alliance forces, as well as a higher degree of interaction with headquarters within the NATO command structure. The development of such capabilities requires the creation and preparation of HQ modules at the operational and tactical level in advance. This will allow, if necessary, to form autonomous headquarters to conduct a separate operation or headquarters modules to be integrated into the NATO headquarters.
- To rethink views about the purpose and structure of the country's defense leadership, command, and control system and, in particular, the system of command and control of the armed forces and building new capabilities. Current trends in military operations require that this system be developed as a command, control, communications, computer, intelligence, surveillance, and reconnaissance (C4ISR) system. It must be able to protect itself from unauthorized access to information, as well as to affect the opponents' commands. This will enable the achievement of information superiority and ensure the deployment of the full operational capabilities of the armed forces. Such capabilities will provide commands at all levels with the ability to acquire, process and analyze intelligence information from all available sources. It will also ensure timely decision-making and the spread of directives and orders throughout the chain of command.

### *C. Technological upgrade*

The technological direction for the improvement of the country's defense leadership, command and control system implies the improvement of the technical architecture, as well as the increase of the efficiency, security and capabilities of the communication and information systems, for the collection, analysis, processing and delivering of information through modern technologies.

The construction of such a complex system includes the construction of surveillance and intelligence systems, reconnaissance systems, information processing systems that ensure the reception, processing and transmission of timely and adequate information between management bodies and their subordinate structures in real time, ensuring reliable operational picture and its transmission to the respective users.

The analysis of the technological provision of the system for management, command and control of the country's defence shows that the main directions for the development of communication and information systems could be:

- provision of strategic, operational, and tactical communications throughout the country. The deployed communication and information network for stationary military support was implemented as part of the country's peacetime preparation. Due to a number of reasons, it does not provide full coverage of the entire country. This requires additional mobile CIS resources to be provided, as well as to use the services provided by the country's unified electronic communication network.
- creation of conditions for technical and functional integration of the telecommunication and information systems of the armed forces and non-military components into a unified C4ISR system. The communication and information system is built on the basis of the networks of the telecommunications operators and the separate information networks of the Government, the Ministry of Defense, other central and regional bodies of the executive power. The experience of the interaction of the formations of the armed forces with elements of the non-military component has shown that the flow of the necessary information is not always guaranteed. On the one hand, the procedures for the exchange of information are not fully detailed, and on the other hand, the technical means available to the formations of the armed forces and the structures of the non-military component are not fully compatible and make it difficult, and sometimes impossible, to exchange information. This leads to difficulties in clarifying the situation, creating common operational picture and making adequate decisions. Therefore, the construction of an integrated unified C4ISR system will ensure

an adequate distribution of responsibilities for receiving and providing information. Also, the presence of such a system will ensure technical compatibility between the individual elements of the defense system, thus improving the exchange of information between military and non-military components.

- achieving interoperability with the NATO command structure. Interoperability of the armed forces' C4ISR systems is of particular importance. In general, interoperability contains three elements: technical compatibility - insists different technical systems to be able to exchange data between each other based on common technical standards for collection, processing and exchange of information; semantic compatibility – requires same semantic content of the exchanged data to be used; and organizational compatibility – which means common procedures for data exchange and processing to be introduced.

#### CONCLUSION

In conclusion, it should be said that the establishment and development of the leadership, command, and control

system of the country's defence in peacetime, in crisis and in wartime is essential for the effective and efficient functioning of the national security and defence system.

The optimization of this system is an objective process, which is dictated by the process of transformation of the armed forces and the extremely rapid development and introduction of new technologies in the military sphere. Gaining success in improvement of the leadership, command, and control system of the country's defence is closely dependent on the economic resources of the country and defence capability development plans adequacy. It largely depends on the skills of the state and military governing bodies, both to organize and to persistently pursue the achievement of the set goals.

The problems of building and transforming the system for leadership, command, and control of the country's defence, considered, and analysed in this study, do not fully exhaust the content of the topic. Nevertheless, the proposed material provides a basis for discussions and debates to help improve it.

#### REFERENCES

- [1] Defence Strategy of the Republic of Bulgaria. Sofia, MoD, 2016, p. 10.
- [2] Strategic Defence Review. Political Framework. Online, <https://www.strategy.bg> [Accessed March 6, 2024].

# *Terrorism – a Barbaric Tool and its Disproportionate Counteraction in the Conflict between Hamas and Israel*

**Steliana Yordanova**

National Security Department  
University of Library Studies and  
Information Technologies  
Sofia, Bulgaria  
s.yordanova@unibit.bg

**Ralitsa Yotova**

National Security Department  
University of Library Studies and  
Information Technologies  
Sofia, Bulgaria  
r.yotova@unibit.bg

**Stoyan Boyanov**

National Security Department  
University of Library Studies and  
Information Technologies  
Sofia, Bulgaria  
s.boyanov@unibit.bg

**Stoyan Garov**

National Security Department  
University of Library Studies and  
Information Technologies  
Sofia, Bulgaria  
115-nd@unibit.bg

**Abstract.** Terrorism and its means have been applied since Ancient times, and over the years the human development and technologies have transformed it into a serious threat to the civilians, societies, countries and even to the international security. The globalisation of terrorism demands new approaches for the effective counteraction, in accordance to the dynamically changing security environment of the 21st century. Meanwhile, with the escalation of the conflict between Hamas and Israel, the issue about the terrorism threat took the headlines, both in the information space and at the highest political level. The discussion focuses on the specific methods of combating terrorism and the permissible level of violence that should be applied in this fight.

This paper seeks to answer important questions regarding security by presenting an analysis of some basics concerning the phenomenon of "terrorism". For this purpose, the applied methods of the research include careful examination of terrorism's evolution throughout history, the factors that have influence over terrorists' attitude, the motivation which fuels one's decision to become a part of a terrorist group and its most striking recent manifestation. Furthermore, the paper puts the emphasis on the necessity of developing new counter-terrorism strategies along with incorporation of the newest technologies in the security sector.

**Keywords:** Fight against terrorism, Hamas-Israel, Terrorism, Security

## I. INTRODUCTION

In the current era of rapid technological changes and globalisation, citizen security is subject to a variety of challenges. One of the most serious and complex problems that stands out in this context is terrorism. This type of crime does not just threaten individuals, but also states as a whole.

Terrorism directly targets the values of freedom, justice and human rights that societies affirm. This report focuses on this phenomenon in a broad way, examining its historical roots on the one hand and its contemporary manifestations, including the ongoing conflict between Hamas and Israel, on the other. The work presents various aspects of terrorism, including the motivation behind terrorist acts, methods to prevent and combat terrorism, and the ethical and legal aspects related to this problem. The analysis covers the international community's response to terrorist threats and how strategies are evolving to keep citizens safe on a global scale.

Terrorism, as a form of violence and extremism, poses a serious threat to the security of citizens in the modern world. Capable of unfolding both locally and globally, terrorism requires complex and multidirectional strategies to prevent and combat it. The history of terrorism, the factors that facilitate its development, and the impact on society and citizens are analyzed.

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8222>

© 2024 Steliana Yordanova, Ralitsa Yotova, Stoyan Boyanov, Stoyan Garov.

Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

## II. MATERIALS AND METHODS

This research implements several methods in its pursuit of determining the phenomenon of terrorism and its actual state as a serious threat for security. The applied methods include a deep analyses of the up-to-date scientific knowledge on the subject of terrorism, the fundamental theoretical basis gathered throughout the decades by numerous researchers, experts and scientists, along with a profound discussion on the most recent terrorist event with significant consequences for the international security, such as Hamas' attack on Israel and the following armed conflict.

The authors have gone through the steps of observation and information gathering, fact-checking the information and the reliability of the sources, analysis of the data and creating hypothesis. Based on the conducted research conclusions have been made about the history, nature, actual state and future of terrorism and the fight against this phenomenon.

## III. RESULTS AND DISCUSSION

### A. History of terrorism

Terrorism as we know it today finds its roots in the history of humanity. From the early forms of political terrorism in the Roman Empire to the religious conflicts of the Middle Ages, terrorist activity has passed through various stages and taken a variety of forms. In the 19th century, with the development of national movements, terrorism took on new dimensions. Anticolonial struggles, the revival of national ideas and political revolutions set the stage for the modern form of terrorism.

In the 20th and 21st centuries, terrorism became a global phenomenon. Terrorist groups such as al-Qaeda, ISIS and their Latin American and Asian counterparts are expanding their reach and influence through the use of new technologies and social networks. Unlike in previous periods, they can now coordinate their attacks and mobilise followers around the world. In this sense, the phenomenon of terrorism has also globalised.

The study of the history of terrorism provides a context for understanding the causes and motivations behind contemporary terrorist actions. For example, religious conflicts in the Middle East and political instability in certain regions are often at the root of terrorism. Understanding this context should aid the process of formulating strategies to prevent future incidents and address threats to citizen security.

### B. Causes of terrorism

Terrorism, as a complex and multi-layered phenomenon, finds its roots in various areas of human activity. One of the key tasks in analyzing this problem is to consider the multiple factors that can support the development and "flourishing" of terrorist groups.

Among the social factors that fuel terrorism, social injustice, poverty and discrimination stand out. People who feel rejected by society or are victims of socio-economic inequalities are more likely to join terrorist groups in search of meaning and change.

Political factors also play an important role in the development of terrorism. Failed or unstable

governments, ethnic or religious conflicts, crises regarding the national identity and the inability to reach agreement and compromise can create an environment conducive to the terrorist rise.

Religious beliefs are also an important factor in motivating terrorists. Religious extremists often use versions of religious doctrines to support their goals and actions. In this context, it is essential to distinguish between religious belief and committing violence in the name of that belief.

The combination of these factors affects the individual and causes him to seek alternative forms of expression, often through violence. Appropriate counter-terrorism strategies should address the roots of these problems, offering comprehensive and sustainable solutions.

### C. Terrorist groups. Motivation and methods.

Terrorist groups operating today represent a diverse landscape of ideologies, goals and methods. Studying these organizations is key to understanding the terrorist landscape and building effective strategies to deal with such entities.

Of the terrorist groups that focus on religious motivations, Al-Qaeda is one of the most notorious. Established in 1988, this group has been linked to numerous terrorist attacks, including the September 11th, 2001 attacks in the United States. Another influential group with religious ambitions is ISIS, which in recent years has been the main terrorist organisation in the Middle East and Africa.

Political terrorism also remains a factor in the modern world. Such groups often pursue goals such as changing power, changing political systems or national independence. Various separatist and communist groups operate in different parts of the world, using terrorist methods to achieve their goals.

Modern terrorism also involves the use of new technologies and methods. The Internet and social networks have become a platform for new membership, propaganda and coordination of terrorist activities. Cyber-attacks have also become a commonly used means of exerting influence and creating chaos.

Understanding the motivations, methods and objectives of terrorist groups is a key element of combating this type of threat. Effective counter-terrorism strategies must adapt to the changing nature of terrorist activity and include close monitoring, intelligence and cooperation at the international level.

### D. Impact on citizens and society

Terrorist attacks have a lasting effect on citizens and society as a whole. Individuals directly affected by these events often experience deep emotional trauma, such as fear, helplessness and concern for the future of society.

On a psychological level, terrorist attacks create an atmosphere of uncertainty and tension. People face the challenge of rebuilding their sense of protection and stability, which can lead to changes in behaviour, perspective and attitude towards others. The growth of fear can undermine trust in institutions, increasing



tensions and divisions. As a result, societal values face challenges.

The impact of terrorism is not limited to the timing of the attack. Long-term effects include changes in security legislation, increased surveillance and stricter protection measures. However, all of this can lead to further challenges to individual liberty and civil rights, raising new debates about the balance between security and personal independence.

Therefore, understanding the impact of terrorism on citizens and societies is a key factor in formulating strategies to prevent and deal with this serious threat, because as Mr. Slavcho Velkov says "terror is fear and dread". In their brutal activity, terrorists are guided by the ancient Chinese proverb "Kill one, scare a hundred", as well as by the Arab military doctrine - "Victory in a war is not measured by the number of killed and wounded, but by the number of the scared".

#### *E. Fight against terrorism*

Combating terrorism requires a coordinated and multidirectional effort by the international community and national governments. One of the main strategies is to develop effective methods to prevent terrorist acts. This includes maintaining a high degree of vigilance and alertness, as well as developing intelligent systems to counter terrorist threats.

In the area of terrorism prevention, education and awareness play a crucial role. The development of educational programmes aimed at understanding the roots and consequences of terrorism can help prevent the recruitment of new members and promote peaceful solutions to conflicts.

Cooperation between different countries and organisations is also essential in the fight against terrorism. The exchange of information and the coordination of efforts to combat the financing of terrorist groups are vital. Terrorism knows no borders, and effective strategies must be coordinated and supported by the international community.

The response to terrorism also includes control of the internet and social networks, which are often used to recruit and plan terrorist activities. In this sense, a key element of the prevention of terrorist acts from materializing should be the research of the behavior of the nowadays information users. For example, such strategy implements the task to determine to what degree people use mobile devices to read, learn and access information resources. The free and almost uncontrollable access to different kinds of information facilitates the radicalization, especially amongst the marginalized groups and the minorities if they feel neglected or threatened [1]. The development of tracking and surveillance technologies can help detect and intercept these threats before they become a reality.

Finally, the approach to tackling terrorism must be balanced, providing security without neglecting respect for fundamental rights and freedoms. Strategies must be adapted to the changing conditions and incorporate the wide range of factors that influence the dynamics of terrorism globally.

#### *F. The conflict between Hamas and Israel – a barbaric attack and a disproportionate counteraction?*

The insidious and devoid of any humanity terrorist attack carried out by the Hamas group against Israel on October 7th 2023 has once again brought the terrorist security threat to the world's attention. In addition, the aggression in question has escalated tensions both throughout the Middle East and at a global level. An unprecedented response by the Israeli State has followed, involving the mobilisation of enormous human and technological resources in order to conduct a ground military operation in the Gaza Strip and eliminate Hamas and its leaders.

Undoubtedly, the attack carried out by Hamas militants has achieved its objective of both striking turmoil and fear into the hearts of the citizens and, on the other hand, provoking such a military response from Israel as to draw the attention of the international community to the fate of the Palestinian people and their status.

The negative security implications for citizens confirm the principles and modus operandi of terrorist groups outlined earlier in the report. Many Israelis lost their lives during the initial attacks, while hundreds were kidnapped by the terrorists. To this day, a significant number remain hostages, used by Hamas as bargaining chips for a pause in the fighting, for example.

The reaction of the international community to the conflict has been and continues to be interesting. Initially, quite in the spirit of humanity, compassion and empathy, most world leaders expressed their deep outrage at the terror of Hamas and showed strong support for the Israeli people. However, when the intense shock wore off and Israel launched its ground operation (accompanied by massive bombardment and artillery fire), and especially when the results of these actions began to be made public in the public space and on social media, it seemed that public opinion in large parts of the world gradually began to tilt in the other direction.

Hamas is now unquestionably reaping the fruits of its "labor." Public space, the mass media, the Internet and social networks are filled with images of destroyed buildings, destitute Palestinians, and an unspecified but certainly large number of civilian casualties. According to some figures from medical officials in Gaza, the death toll from the relentless bombardment exceeds 25 000 [2].

The anguish and suffering of the Palestinians is not only front and centre in the news, but is also the subject of discussions, conferences and meetings at the international level. Personally, the Pope, who recently met both with Israeli relatives of hostages held by Hamas and with Palestinians with families in Gaza, has expressed his concern about what is happening, of which his words are ample testimony: "This is what wars do. But here we have gone beyond wars. This is not a war. This is terrorism" [3].

Naturally, a reaction followed from Israeli officials who repeatedly stated their firm position that there can be no equivalence between Hamas, which is a terrorist organisation and uses civilians as human shields, and Israel, which protects civilians. According to Israel, the starting point in this conflict is terrorism and it must be

eradicated [4]. However, too few answers remain to the real questions, such as what factors gave rise to the creation and development of Hamas as a terrorist organisation. Too often, national governments and the international community grapple with the consequences rather than focusing on identifying and preventing threats of this nature.

It is from this national perspective that Israel is within its rights to use force to protect the security of its citizens as well as its own existence. On the other hand, however, perhaps the overreaction has had more negative effects than anyone imagined. The UN General Assembly has demanded, by a resolution adopted by an overwhelming majority, a humanitarian ceasefire in the Gaza Strip. The manner of the vote is significant - 153 votes in favour, 10 votes against and 23 abstentions. On the one hand, this is a strong demonstration of global support for an end to the war between Israel and Hamas. On the other hand, it could be interpreted as a growing isolation of the US and Israel from the international community regarding the conflict [5].

The analysed case raises more questions than answers. What should be the counter-terrorism response in the 21st century? How should citizens be protected from terrorist acts? How far does the law of force go? All these questions are deeply causally linked to the future evolution of the terrorist threat and the security challenges that societies and states will face in the years and decades to come.

#### G. Future Challenges and Developments

As the fight against terrorism evolves, new challenges and possible developments arise that must be taken into account when formulating strategies for the future. One important future challenge is the adaptation of terrorist groups to changes in technology. The use of encryption, anonymous platforms and other technological innovations may make detecting and countering terrorist activities more difficult.

The global nature of terrorism calls for improved international cooperation. Countries and organisations need to strengthen information exchange, coordination of actions and sharing of good practices. The establishment of effective international counter-terrorism standards and laws is essential.

At the same time, attention must also be focused on preventing radicalisation and the inclusion of new members. Education and social inclusion programmes must be developed to provide alternatives for those at risk of joining terrorist groups.

In the future, the role of tracking and monitoring technologies will continue to grow. Intelligent systems for analysing and processing big data can help identify potential threats before they materialise. However, creating a balance between the need for security and respect for privacy must be put at the forefront.

#### IV. CONCLUSIONS

Terrorism, as a threat to the security of citizens, continues to challenge the global community and national governments. Its complexity and dynamics require the constant development of strategies and means to address

this serious threat. Through the lens of history, we have analyzed the evolution of terrorism from various ideological, political, and religious perspectives.

Awareness of the social, political and economic factors that fuel terrorist activities is critical to building sustainable prevention strategies. Also, the impact on citizens and societies, as well as future challenges, require an integrated and balanced approach that combines security with respect for fundamental rights and freedoms.

In the fight against terrorism, international cooperation and information sharing play a key role. Current events in recent months, and specifically the armed conflict between Hamas and Israel, raise questions about the means by which counter-terrorism must be carried out in order to be effective.

It has been proven that neutralizing the terrorist threat is impossible only through retaliatory violence. The creation of intelligent systems and the use of technology to prevent terrorist acts must be developed in parallel with educational and social programmes to combat radicalisation.

Looking forward, strategies to fight terrorism will need to be adaptive, sustainable and global. Cooperation and innovation will be key factors in building a safer and more sustainable world where citizens can live without fear of terrorist threats.

#### ACKNOWLEDGMENTS

This work 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] I. Peteva, S. Denchev and E. Tsvetkova, Impact of Mobile Technology on Learning and Library Policies. In: Guarda, T., Portela, F., Diaz-Nafria, J.M. (eds.) *Advanced Research in Technologies, Information, Innovation and Sustainability*. ARTIIS 2023. Communications in Computer and Information Science, vol. 1937. Springer, Cham., 2024, pp 102–115. [https://doi.org/10.1007/978-3-031-48930-3\\_8](https://doi.org/10.1007/978-3-031-48930-3_8) Print ISBN 978-3-031-48929-7; Online ISBN 978-3-031-48930-3
  - [2] Al Jazeera and news agencies, "Gaza death toll surpasses 25,000 as Israel escalates assault", January 2024. [Online]. Available: <https://www.aljazeera.com/news/2024/1/21/gaza-death-toll-surpasses-25000-as-israel-escalates-assault> [Accessed: Feb. 2, 2024].
  - [3] P. Pullella, "Dispute erupts over whether pope called Gaza situation a 'genocide'", November 2023. [Online]. Available: <https://www.reuters.com/world/pope-says-conflict-between-israel-hamas-has-gone-beyond-war-terrorism-2023-11-22/> [Accessed: Feb. 8, 2024].
  - [4] BTA, „ANSA: Papa Frantsisk ne postavya Izrael i "Hamas" na edno i sashto nivo, zayavi predsedatelyat na Italianskata episkopska konferentsia Mateo Dzupi.“, November 2023 [Online]. Available: <https://www.bta.bg/bg/news/world/574616-ansa-papa-frantsisk-ne-postavya-izrael-i-hamas-na-edno-i-sashto-nivo-zayavi> [Accessed: Jan. 30, 2024].
- [BTA, „АНСА: Папа Франциск не поставя Израел и "Хамас" на едно и също ниво, заявя председателят на Италианската епископска конференция Матео Дзупи.“, November 2023 [Online]. Available: <https://www.bta.bg/bg/news/world/574616-ansa-papa-frantsisk-ne-postavya-izrael-i-hamas-na-edno-i-sashto-nivo-zayavi> [Accessed: Jan. 30, 2024].

- [5] БТА, “ОБНОВЕНА Общото събрание на ООН одобри с огромно мнозинство резолюция, с която се иска хуманитарно прекратяване на огъня в ивицата Газа.”, December 2023 [Online]. Available: <https://www.bta.bg/bg/news/world/586047-obshoto-sabranie-na-oon-odobri-s-ogromno-mnozinstvo-rezolyutsiya-s-koyato-se-i> [Accessed: Feb. 6, 2024]
- [БТА, “ОБНОВЕНА Общото събрание на ООН одобри с огромно мнозинство резолюция, с която се иска хуманитарно прекратяване на огъня в ивицата Газа.”, December 2023 [Online]. Available: <https://www.bta.bg/bg/news/world/586047-obshoto-sabranie-na-oon-odobri-s-ogromno-mnozinstvo-rezolyutsiya-s-koyato-se-i> [Accessed: Feb. 6, 2024]
- [6] K. Kazakov, Terorizmat, kato strategicheska zaplaha. Godishna universitetska nauchna konferentsia – NVU „Vasil Levski“, 20 – 21 oktombri 2016, ISSN 1314-1937. COBISS.BG-ID 1237830884
- [К. Казаков, Тероризмът, като стратегическа заплаха. Годишна университетска научна конференция – НВУ „Васил Левски“, 20 – 21 октомври 2016, ISSN 1314-1937. COBISS.BG-ID 1237830884]
- [7] A. Zahariev, Etno-religioznite otnoшения - klyuchov faktor za proyavi na terorizam. Sbornik s dokladi ot Nauchna konferentsia "Aktualni problemi na sigurnostta" NVU "V. Levski". 2023, s. 372-380, ISSN 2367-7473.
- [А. Захариев, Етно-религиозните отношения – ключов фактор за прояви на тероризъм. Сборник с доклади от Научна конференция „Актуални проблеми на сигурността“ НВУ „В. Левски“. 2023, с. 372-380, ISSN 2367-7473]
- [8] G. Stoyanov, Riskove i zaplahi za vatreshnata sigurnost na Republika Bulgaria. Sofia: Izd. Fondatsia Natsionalna i mezhdunarodna sigurnost, 2020
- [Г. Стоянов, Рискове и заплахи за вътрешната сигурност на Република България. София: Изд. Фондация Национална и международна сигурност, 2000]
- [9] T. Trifonov and A. Peychev, Terorizmat. Teoretichno izsledvane. Sofia: Izd. Fondatsia „Natsionalna i mezhdunarodna sigurnost“, 2003. ISBN: 954-90695-6-7
- [Т. Трифонов и А. Пейчев, Тероризмът. Теоретично изследване. София: Изд. Фондация „Национална и международна сигурност“, 2003. ISBN: 954-90695-6-7]
- [10] I. Palchev, Teror. Sofia: Izd. na BAN „Prof. Marin Drinov“, 2018. ISBN 978-954-322-918-5
- [И. Палчев, Терор. София: Изд. на БАН „Проф. Марин Дринов“, 2018. ISBN 978-954-322-918-5]
- [11] O. Zagorov and N. Yordanov, Terorizmat. Psihologia. Ideologia. Geopolitika. Sofia: „Voenno izdatelstvo“ EOOD, 2007. ISBN 978-954-509-374-6
- [О. Загоров и Н. Йорданов, Тероризмът. Психология. Идеология. Геополитика. София: „Военно издателство“ ЕООД, 2007. ISBN 978-954-509-374-6]
- [12] Global Terrorism Database. [Online], Available: <https://www.start.umd.edu/gtd/> [Accessed Feb 9, 2024]
- [13] Borba s terorizma. V ofitsialnata internet stranitsa na Ministerstvo na vashnite raboti na Republika Bulgaria. [Online], Available: <https://www.mfa.bg/bg/3103> [Accessed Feb 9, 2024]
- [Борба с тероризма. В официалната интернет страница на Министерство на външните работи на Република България. [Online], Available: <https://www.mfa.bg/bg/3103> [Accessed Feb 9, 2024]

# Implying cybersecurity skills for public administration employees

**Radoslav Yoshinov**

Laboratory of telematics  
Bulgarian Academy of Sciences  
Sofia, Bulgaria  
yoshinov@cc.bas.bg

**Monka Kotseva**

Laboratory of telematics  
Bulgarian Academy of Sciences  
Sofia, Bulgaria  
mkotseva@cc.bas.bg

**Anastas Madzharov**

Institute of Robotics "St. Ap. and  
Gospeller Matthew"  
Bulgarian Academy of Sciences  
Sofia, Bulgaria  
a.madzharov@ir.bas.bg

**Neda Chehlarova**

Institute of Robotics "St. Ap. and  
Gospeller Matthew"  
Bulgarian Academy of Sciences  
Sofia, Bulgaria  
nedachehlarova@ir.bas.bg

**Abstract.** The results of a conducted study on the knowledge and skills of representatives of the public and local administration regarding cyber security in modern digital work processes are presented. The survey was conducted in 2023 in the Republic of Bulgaria. The analysis includes a comparison of the data with those of a similar survey of employees in the public administration in 2020.

**Keywords:** cybersecurity, cyberethics, digital competence, public administration, employees

## I. INTRODUCTION

The use of ICT tools as a fundamental support of traditional processes related to management and administration has led to the term e-governance (e-government). This term does not have a clear definition, but we will accept "the use of information and communication technologies (ICT), especially the Internet, as a tool to achieve better governance". Data is now an integral part of every sector and function of government – as important as physical assets and human resources, and its management requires special attention and expert action [1]. In order to improve the digital competencies of employees in government structures, it is essential to have a prepared and well-informed administration [2] - [5]. This requires drawing a clear picture of the current state and creating a plan for progress that meets societal needs [6] - [10].

Here are analyzed the preparation and awareness of employees of the public administration, comparing the results with a similar study conducted in 2020 [11]. A part of the questions was reserved in order to report whether there is development on basic topics, such as security, problem solving, communication between individual units

and citizens. The questions from 2020 have been adapted and the data in the comparative analysis is based on the number of respondents. Another part was supplemented by taking into account the new realities of progress in digital transformation and the possibilities of using artificial intelligence for the modernization and overall improvement of the functioning of public administration.

## II. MATERIALS AND METHODS

The study involved two groups of public administration employees, with the first study conducted during the COVID-19 pandemic in 2020 and then repeated in 2023. Both surveys were anonymous and voluntary, and therefore different numbers of respondents participated in the different periods, with the number of participants in the first survey being over 175, and in the second over 75.

## III. RESULTS AND DISCUSSION

The age profile of the two groups of respondents is similar and includes mostly respondents between 30 and 65 years old "Fig 1".

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8238>

© 2024 Radoslav Yoshinov, Monka Kotseva, Anastas Madzharov, Neda Chehlarova.

Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

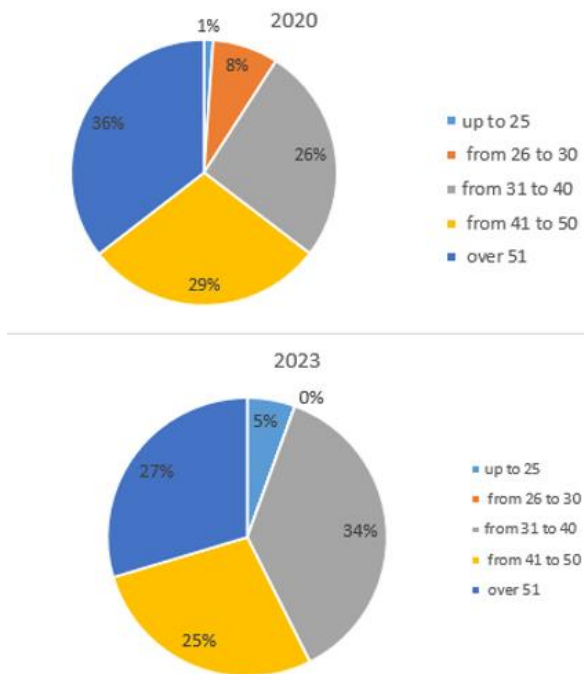


Fig. 1 Age distribution of participants in 2020 and 2023.

The distribution by gender is similar, and in the second survey it is noticed that more men took part “Fig. 2”, but again the ratio is 2:1, although according to official statistics the distribution of employees in the administration is even [2].

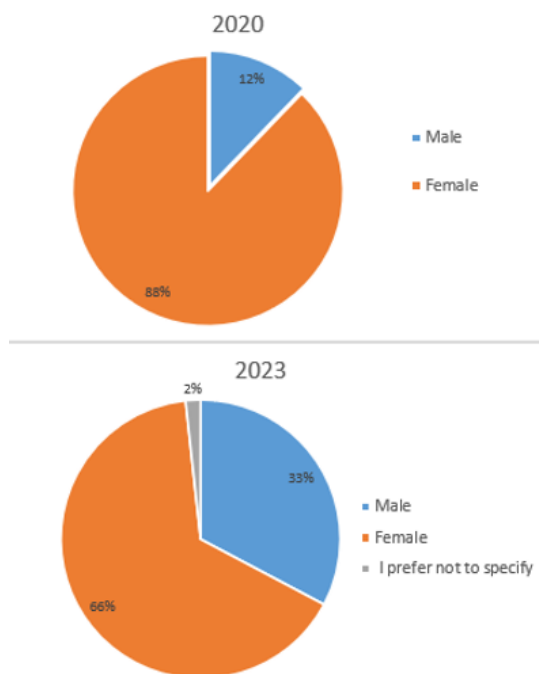


Fig. 2 Gender distribution of participants in 2020 and 2023.

During the crisis related to the spread of COVID-19, a number of activities and administrative services of the central and local authorities were put to the test. We all know that the pandemic caught us off guard and forced public authorities and many businesses to digitize their services, making them easily accessible online [12]. Data from the first survey show that although the Internet was the place for communication, those who answered the question "How much time do you use the Internet for

work?" are 62% of the respondents, and the activities they perform are between 1 and 2 hours. To the question: "After and during the COVID-19 pandemic, did you have to carry out your activity electronically (without direct contact with consumers)?", 69% of the administration answered that they carried out their activity entirely on the Internet, as on 31 % of them had to perform their duties online for the first time. In proportion to the entry of technological innovations into our daily duties, new security problems also arise. By its nature, the concept of information security is of strategic importance for the interests of the individual, society and the state as a whole. In order to be able to achieve higher levels of security in the field of information technology, it is necessary to achieve a higher awareness, both about the threats to information security, and about the methods of combating the threats. This is especially important for people working in public administration. For this reason, the main emphasis in the survey was the questions related to the preparation of the employees in this direction when performing their duties.

It is known that the employees in the administration have access to many and different types of data. One of the most important data protection tools is multi-factor authentication (MFA) [12] - [13]. It uses at least two different components from the categories of knowledge, possession and biometrics for registration. Here are the results of the question: "Are you familiar with (using) any of the listed options for multifactor authentication?" “Fig. 3”:

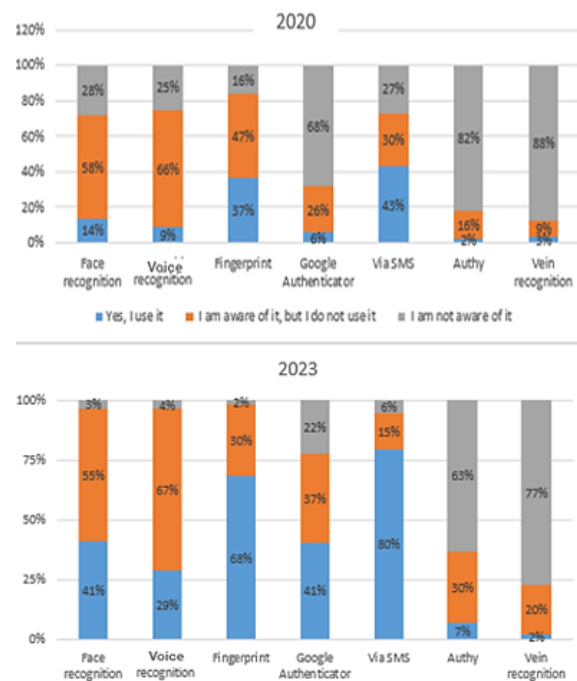


Fig. 3 Are you familiar with (using) any of the listed options for multifactor authentication.

It is noteworthy that, compared to the 2020 survey, the 2023 result shows that most of the specified authentication methods are not unfamiliar, although not all are used. The most common means of protection used are SMS and fingerprint, which have nearly doubled since 2020, with SMS being used by 80% and fingerprint by nearly 70% of respondents. Other responses that show an

increase in employee awareness and knowledge are related to the voice and facial recognition authentication group, which saw a 3-fold increase but maintained non-use rates. Two-factor authentication applications (such as Authy) and biometric vein recognition systems are still unknown and underutilized.

Information security also requires knowledge of possible threats. To the question: "Do you know any of the listed threats related to information security?" the following responses were given shown in "Fig. 4".

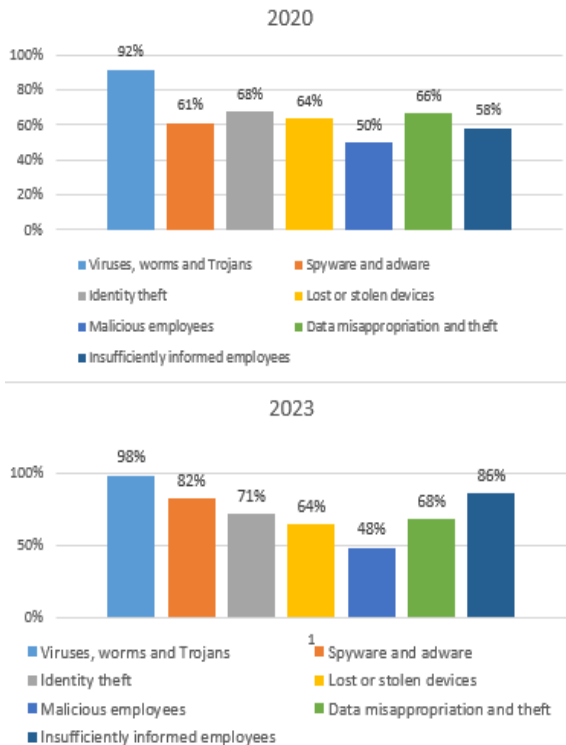


Fig. 4 Do you know any of the listed information security threats.

Viruses, worms and trojans are well known in both surveys, with 100% awareness in the 2023 survey. It is encouraging that some of the listed threats have increased awareness by between 10 - 20% [11]. Lost/stolen devices, malicious employees, and data and identity theft and misappropriation remain at the same levels, with the largest increase in the victimization rate of insufficiently informed employees, which is a natural process accompanying the greater number of services offered in the Internet space.

Another important aspect of security is the reliability of security mechanisms, knowledge and their correct use. Here is the development of responses to the question: "Are you aware of any of the information security threats listed below?" "Fig. 5".

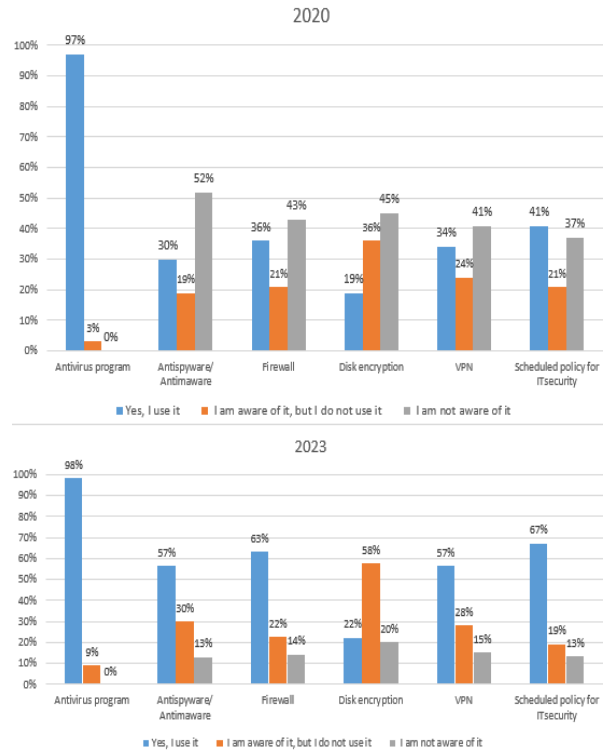


Fig. 5 Which of the following means of protection do you know.

In proportion to virus awareness, the use of anti-virus programs is close to 100%. The use of the remaining means of protection listed in the survey has grown almost twice, which speaks of an increase in the awareness of the respondents [11]. The result of knowledge of data encryption has not undergone significant change and is still not used as a way of prevention. This fact may be due to the fact that most cloud service providers use encryption, but the problem remains when it comes to data on portable or personal media, and the information handled by the government administration is sensitive for all of us.

No less a threat to information systems can be human errors, technical failures or malicious attacks. This was the reason for asking: "How do you solve problems related to ICT technologies?" "Fig. 6". From the results shown, it is noticeable that the percentage of respondents who rely on their own strength to solve problems in the field of ICT has increased. Most employees rely on their knowledge and on friends and colleagues to deal with the problem. Addressing a question to a specialist still maintains its score of around 60%, and delegating responsibility to a specialist has even seen a decrease, although they should be trusted more as they have the knowledge and experience to help resolve complex problems in IT.

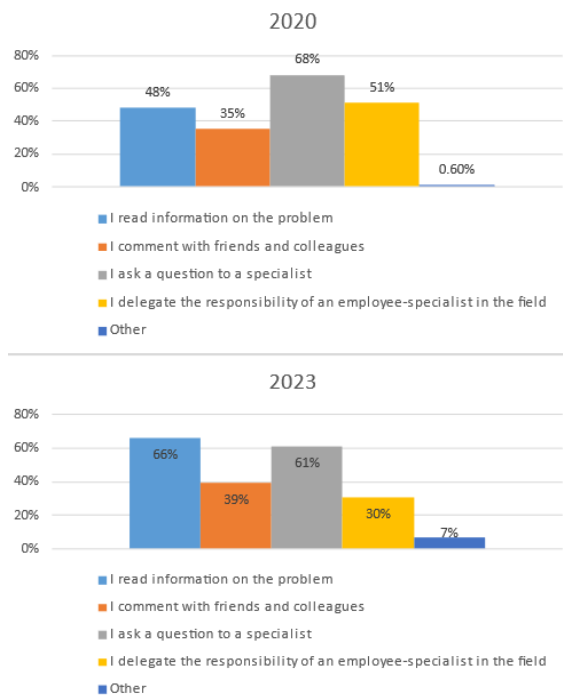


Fig. 6 How do you solve problems related to ICT technologies.

According to an IPA survey to study the level of digital competence of employees in the public administration [14] makes an impression, that employees acquired knowledge during the performance of official duties are twice as many as those who acquired knowledge independently and during on-the-job training (Table 1). Perhaps this also determines the greater confidence in their own abilities than in specialized response.

TABLE 1. DIGITAL COMPETENCE OF PUBLIC ADMINISTRATION EMPLOYEES ACCORDING TO THE IPA REPORTABLE

I am self-taught (I have used resources available on the Internet)	21%
The knowledge I have acquired during the work/ work process	71%
The knowledge I have acquired during on-the-job training	26%
The knowledge I have acquired during extracurricular/additional training	24%

We asked the surveyed participants “Do you think you have been a victim of a cyberincident/cybercrime?”. Answer “Yes” was written by 8 representatives of the public administration. 6 representatives of the public administration answered “No”. The rest indicate that they “don’t know”. One respondent shared: „It’s very possible that my lack of knowledge earlier in life led to a possible data leak - it’s entirely possible that something like that happened, but I haven’t encountered any consequences for myself so far“.

Overcoming difficulties in IT can provide valuable lessons and opportunity for development, but it often takes much longer. That is why every organization needs to have IT specialists who can not only solve technological problems, but also know the problems that the specific department deals with. This saves time, effort and resources, and manages to increase the efficiency of the organization’s work by identifying the most cost-effective solution.

## CONCLUSION

The growing dependence on information and communication technologies in all spheres of human life causes the emergence of vulnerabilities that require proper identification, careful analysis and subsequent removal or limitation. All actors, whether public authorities, private sector representatives or individual citizens, must recognize this shared responsibility, take action to protect themselves and, if necessary, provide a coordinated response to strengthen cyber security.

There is a development of the digital competence of the surveyed public administration employees in the country related to cyber security - prevention, knowledge, protection, application of methods for dealing with cyber threats. From the conducted research, among representatives of the public administration in 2023, compared to that of 2020, there is an increase in the percentage of information security threats that are known. There is also an increase in the values of the used methods and means of protection. At the same time, the percentage of people who do not know the listed protection methods has halved. There is a double increase in 6 out of 7 specified methods of multi-factor authentication used by the respondents. We note that such authentication methods have become a mandatory element when using many of the mobile applications and desktop sites of the banking sector in the country. The increased awareness of the studied group is also considered according to the ways in which they solve problems related to ICT technologies. Respondents have more confidence in their own knowledge to independently solve the problem and/or search for relevant information on it, including by commenting with friends and colleagues. There is a decrease in the percentage of respondents who delegate responsibility to a colleague specialist in the field.

The presented results of the comparative studies in 2020 and 2023 can be used for the adaptation of educational content within the educational process in higher schools, the topics of training for public administration employees, to create the necessary conditions for ethical behavior in the modern working cyber environment.

## ACKNOWLEDGEMENT

This work 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] Department of Economic and Social Affairs, Digital government in the decade of action for sustainable development; UNITED NATIONS New York, 2020. [Online]. Available: [https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20\(Full%20Report\).pdf](https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf) [Accessed: Feb. 22, 2024].
- [2] Report on the state of the administration - 2022. [Online]. Available: [https://iisda.government.bg/annual\\_report\\_file/623\\_319\\_0](https://iisda.government.bg/annual_report_file/623_319_0) [Accessed: Feb. 22, 2024].
- [3] O. Iliev, R. Yoshinov and G. Tsochev, “Verification of user identity and data security in the context of LMS and LCMS,” Mathematics and Education in Mathematics, Proceedings of the Forty-ninth Spring Conference of the Union of Bulgarian Mathematicians, 2020, pp.144-151.

- [4] E. Zhestkova. Subject Information and Educational Environment as Means of Formation of Information and Communication Competence of Future Professionals. *Environment. Technology. Resources. Proceedings of the 11th International Scientific and Practical Conference. Volume II, 2017*, pp. 180-184. <http://dx.doi.org/10.17770/etr2017vol2.2515>
- [5] R. Trifonov, O. Nakov, S. Manolov, G. Tsochev and G. Pavlova, "Possibilities for Improving the Quality of Cyber Security Education through Application of Artificial Intelligence Methods," *International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, 2020*, pp. 1-4.
- [6] Digitalization in training of public administration personnel. © Published by National Institute of Administration on August 2023. [Online]. Available: [https://www.ipa.government.bg/sites/default/files/digitalization\\_in\\_training\\_of\\_public\\_administration\\_personnel\\_2023.pdf](https://www.ipa.government.bg/sites/default/files/digitalization_in_training_of_public_administration_personnel_2023.pdf) [Accessed: Feb. 22, 2024].
- [7] L. Coppolino, S. D'Antonio, G. Mazzeo, L. Romano and L. Sgaglione, "How to Protect Public Administration from Cybersecurity Threats: The COMPACT Project," *32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), Krakow, Poland, 2018*, pp. 573-578.
- [8] R. Trifonov and R. Yoshinov, "Some Security Issues of the Governmental Cloud," *International Journal of Computers. Vol. 1, 2016*, pp. 185- 190.
- [9] R. Trifonov, S. Manolov, R. Yoshinov, G. Tsochev, S. Nedev and G. Pavlova, "Operational cyber-threat intelligence supported by artificial intelligence methods," *Proceedings of the International Conference on Information Technologies (InfoTech-2018), 20-21 September, 2018*, pp 1-9.
- [10] I. Gaidarski. "Some Aspects of Information Security and Cybersecurity Problem Area," *Problems of engineering cybernetics and robotics, Vol. 79, 2023*, pp. 55-66. <https://doi.org/10.7546/PECR.79.23.03>
- [11] N. Chehlarova, G. Tsochev, M. Kotseva and R. Miltchev, "Digital Competencies Of Public Administration Employees Related To Cybersecurity," *Proc. 12th National Conference with International Participation "Electronica 2021", May 27 - 28, 2021*, pp. 1-4.
- [12] G. Tsochev and R. Yoshinov, "Research on Cyber-Physical Systems Security," 1st ed., Sofia, Bulgaria: "Education and Knowledge", 2020, p. 258.
- [13] T. Tagarev, Krassimir, T. Atanassov, V. Kharchenko and J. Kacprzyk, "Digital Transformation, Cyber Security and Resilience of Modern Societies," 1st ed. Springer Cham, 2021, p. 495, eBook <https://doi.org/10.1007/978-3-030-65722-2>
- [14] Project "Digital Transformation in Education - Digital Competence and Learning", financed by Operational Program "Good Governance", co-financed by the European Union through the European Social Fund. [Online]. Available: <https://www.ipa.government.bg/bg/proekt-digitalna-transformaciya-v-obuchenieto-digitalna-kompetentnost-i-uchene> [Accessed: Feb. 22, 2024].

#### SURVEY

- Your age is: (up to 25; from 26 to 30; from 31 to 35; from 36 to 40; from 41 to 45; from 46 to 50; from 51 to 55; from 55 to 60; over 60)
- You are: (Male; Female; I prefer not to specify)
- After and during the COVID-19 pandemic, did you have to carry out your activity electronically (without direct contact with consumers)? (Yes, for the first time; Yes, but I have done it before electronic; No).
- Are you familiar with (using) any of the listed options for multifactor authentication? (Yes, I use it; I am aware of it, but I do not use it; I am not aware of it) (Face recognition; Voice recognition; Fingerprint; Google Authenticator; Via SMS; Authy; Vein recognition)
- Are you aware of any of the information security threats listed below? (Yes; No) (Viruses, worms and Trojans; Spyware and adware; Identity theft; Lost or stolen devices; Malicious employees; Data misappropriation and theft; Insufficiently informed employees)
- Which of the following means of protection do you know? (Yes, I use it; I am aware of it, but I do not use it; I am not aware of it) (Antivirus program; Antispyware / Antimalware; Firewall; Disk encryption; VPN; Scheduled policy for IT security)
- How do you solve problems related to ICT technologies? (I read information on the problem; I comment with friends and colleagues, hoping that they have encountered a similar problem; I ask a question to a specialist; I give up the specific problem; I delegate responsibility to a third party; I delegate the responsibility of an employee-specialist in the field; Other)
- Do you think you have been a victim of a cyberincident/cybercrime? (Short answer text).



# *Conceptual Model of an Automated System for Processing Information From Open Sources and Detecting Information Deviations*

**Ralitsa Yotova**

*University of Library Studies and Information Technologies,*

*National Security Department*

*Sofia, Bulgaria*

*r.yotova@unibit.bg*

**Abstract.** This research focuses on the development of a Conceptual Model of an automated system for processing information from open sources and detecting information deviations. The purpose of the model is to provide a framework within which to develop and implement technologies and methods that will enable the system to effectively collect, process, and analyze information from a variety of sources.

The automated system concept is intended to improve the efficiency and accuracy of intelligence work by using automated methods and algorithms to analyze large volumes of data and information. To achieve this goal, the components and functions of the system will be discussed, as well as the ways in which they interact.

The model proposes an integrated approach combining different technologies and methods to achieve efficient information processing and detection of deviations. The proposed system has the potential to be applied not only in the security sector, but also in various fields such as business, finance, medicine, and others where information from open sources is essential for decision making.

**Keywords:** *open sources, information, model, analysis*

## I. INTRODUCTION

It is definitively clear that in today's world, where information plays an ever-increasing role, intelligence faces significant challenges in the collection, processing and analysis of information gathered from open sources.

Advances in modern open source intelligence, data mining, machine learning, digital forensics, and most importantly, the increasing computing power available for commercial use, are enabling OSINT practitioners to significantly accelerate and even completely automate intelligence collection and analysis.

As the information space expands, the OSINT toolset is constantly changing and improving. This statement is not at all surprising given that open source information has continually increasing volume. To meet this challenge, more and more effective techniques are being developed and introduced which, together with the development of artificial intelligence systems, make productivity inextricably linked to the quality of the technical tools used by analysts.

Undoubtedly, conventional methods of collecting and processing information are becoming increasingly inefficient and unable to respond to the rapidly changing environment. For this reason, the implementation of automated systems to deal with the collection, processing and analysis of information from open sources is becoming more and more necessary. [2-6]

Based on advanced algorithms and operating models, such systems can process and analyse large volumes of data and information faster and more efficiently, assisting the human factor. Moreover, they make detecting information deviations, filtering relevant information and extracting more accurate and up-to-date data an instantaneous process. These types of systems have the potential to change the way security services operate and support their activities many times over. [7-8]

Not only in the field of intelligence, but also for the implementation of various activities that characterise the current social reality, time is of the essence and constant monitoring and timely response in decision-making are vital. [9-12] With the increased levels of network connectivity and constant interaction that underpin the modern information society, monitoring, collecting and analysing data and information from different sources becomes an almost impossible mission without the capabilities of information technology to support these processes. [13-16]

*Print ISSN 1691-5402*

*Online ISSN 2256-070X*

<https://doi.org/10.17770/etr2024vol4.8230>

© 2024 Ralitsa Yotova. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

A major challenge in the processing and analysis of open sources becomes the ability to convert into relevant information large volumes of data, which in most cases are unstructured, unorganized, come from questionable sources, in different forms and from different channels of information. The development and implementation of specific methods and tools to create, validate and improve databases tailored to intelligence needs becomes a high priority.

## II. MATERIALS AND METHODS

In this regard, the proposed conceptual model is based on the well-known JDL-model. For this reason, its architecture is rather functional and aims at the operational provision of a segment “necessary operational capabilities” [1] of the central key organizational competences of the state power, directly concerning the structures of the national security system, among whose main activities is the information analysis.

As a methodology of development, the Conceptual Model is constructed of distinct modules according to the specificity of information analysis activities, which partially overlap with the methodology of other methods of structured analysis.

All the components and sub-processes of the structural and functional scheme of the model are appropriately integrated into a common system for generating new information, as well as for simulation modelling, research and training.

The model aims to represent the totality of all components and subsystems and their interaction in the implementation of analytical methods on information from open sources as a basis for the development of an information processing system. Reducing the involvement of the human factor in the processing processes will reduce subjectivity and increase objectivity in the results obtained as a consequence of the automated system.

Based on what has been presented so far, a possible implementation of an algorithm for the operation of the automated system proposed by the Conceptual Model for processing information from detected sources and for detecting information deviations generally includes the following steps:

### 1. Collecting a training data set

The system collects a training data set that includes information from open sources classified as “normal” or “deviating”. This data set is used to train a Bayes classifier.

### 2. Building a Bayes model

The system builds a Bayes model based on the training data set. This model is used to determine the probabilities of occurrence of various features or attributes in the normal and outlier data.

### 3. Classification of new data

After successful training of the Bayes model, the system can classify new data from open sources. This is done by calculating the probabilities of occurrence of various features or attributes in the new data and using the Bayes model to determine the classification of this data as “normal” or “deviating”.

### 4. Detection of information deviations

The system uses the classification results of the new data to detect informational deviations. If the new data is classified as “deviating”, the system may generate a warning or take other actions to signal the presence of a deviation.

## III. RESULTS AND DISCUSSION

The presented methodology and tools of the research allowed to present the Conceptual Model of an automated system for processing information from open sources and detecting information deviations with the following functional characteristic:

The “entrance” of the information processing system with “dashed circles” in green color represents the movement of information from the information environment to the system. These circles present an array of information representing the interrelationships between events and facts occurring in the objectively existing environment and the occurrence of a problem in the organizational structure, for the purpose of which a solution needs to be found following the application of the Content Analysis method. The graphic shows the process (flow) of information from the objectively existing environment to the information processing and analysis system (Fig. 1).

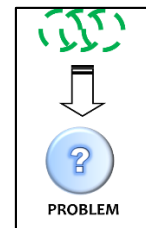


Fig. 1. Entrance

In Module 1 “Areas of Application”, the interplay and intertwining of the different areas of human activity that carry out information and analytical work is presented through an iridescent coloured sphere. Thus, the role of the Content Analysis method and the possibilities of its automation in the study of individual processes and events in the fields of national security, politics, media, and medicine are shown. Since Content Analysis is a widely applicable method, the possibility of applying it in other areas of science and human activity is also shown (Fig. 2).

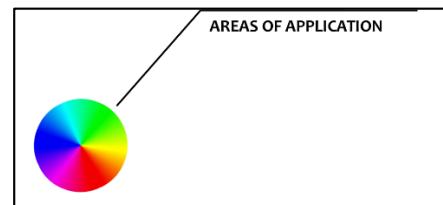


Fig. 2. Areas of Application

Component 2 “Expert” is a core component of the Conceptual Model. Considering the role of the expert in the model, it has basic control functions, which consist not only in controlling and monitoring the operation of the automated system, but also to monitor the flow of information processing in the individual stages. The expert’s knowledge and experience play an important role in deciding how to deal with the information received and, in particular, whether to run the automated information

system and whether it is suitable for processing the information in question.

An open sources monitoring system is presented in Module 2 by means of a “colour sphere” (Fig. 3). It is a set of technical means (so-called “sensors”) by which information is gathered from a self-updating database containing detected information sources. Through them, it provides sensitivity (sense, sensibility) to the movement of the detected sources, and in interaction with them it converts its response into signals, which are coded messages about quantitative or qualitative characteristics of the state of these sources. Its essential characteristic contains a set of specific technical means, representing sensors and sources of information, which provide objective information with respect to the objectively existing environment.

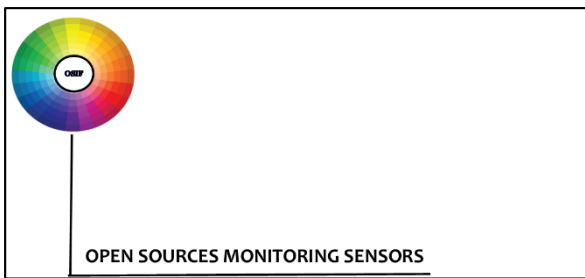


Fig. 3. Open sources monitoring sensors

The main task of the sensor system is to monitor the detected sources of information, thus collecting and summarizing the readings of the different sensors (the types of detected sources) in order to obtain an overall picture of the environment that meets the requirements of completeness, reliability, accuracy, reliability and objectivity.

Module 3 (Fig. 4) presents the integrated databases in the automated information processing system.

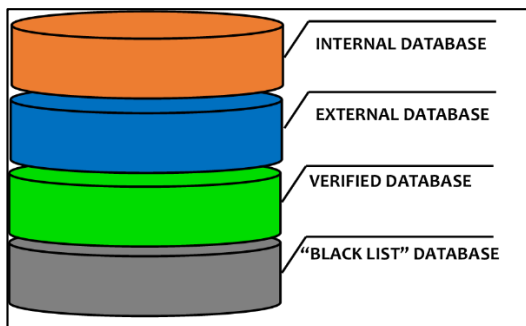


Fig. 4. Database

Databases are essential for the final evaluation and verification of information. In its autonomy and after comparison with the original, basic information, the automated system stores the generated information that does not meet the criteria of information reliability and source reliability in a “black list” database. Thus, the system will subsequently match the collected information with the existing information in the database and not use it.

The guiding task here is the overall monitoring and maintenance of the currency of the sources reviewed and

the data used, which should ensure informed decision making at the expert end of the chain.

Subsystem 1 “Defining Analysis Sources” presents the first stage of the application of the Content Analysis method in the automated system, where the selection of the main information sources to be fed into the automated system is performed. This stage of the information analysis is an important part of the overall information analysis process that is the Content Analysis method. The definition of the basic text (data) that the system will process also determines the quality of the results obtained at the end. Both in this stage and in each subsequent stage, the expertise and knowledge of the expert is paramount in controlling the overall system and its effectiveness (Fig. 5).



Fig. 5. Defining analysis Sources

Subsystem 2 of the Conceptual Model presents Stage 2, which shows the process of selecting information from the common set of open sources of information. The presented graphic (Fig. 6) shows the process of reviewing and selecting specific information in the system relevant to the problem at hand. In this way, the sources of information that are not suitable for the purpose of the study are eliminated, and only those that meet the content constraints set in the system for the most relevant data are extracted.

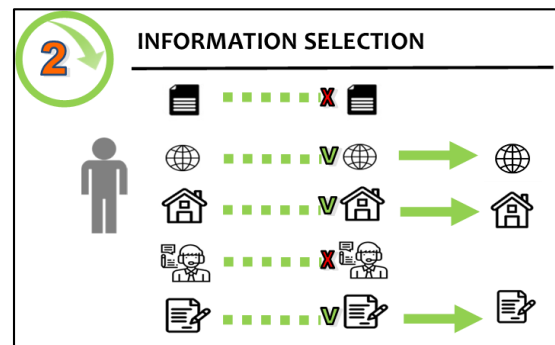


Fig. 6. Information Selection

Subsystem 3 also presents the next stage of automated Content Analysis, which shows the process of identifying the units for analysis. As can be seen in Fig. 7, these units can be words, paragraphs, sentences, symbols or specific topics. By defining predefined criteria for the selection of the units of analysis by the expert, only the information that meets the demand and is suitable for further processing is extracted. Those units that are not large enough to have any semantic value or are too long are dropped from the system, resulting in ambiguities that can cause the system to fail or lock up. An important point at this stage in the search for qualitative entities is that they must be easy to identify and must be contained in a large

enough volume of information so that identification can take place.

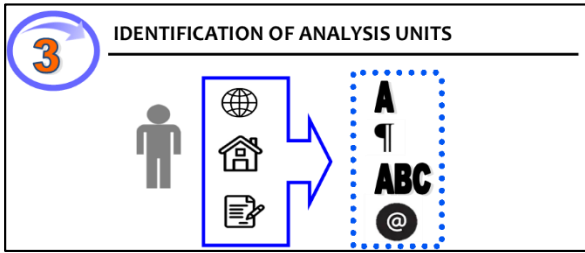


Fig. 7. Identification of Analysis Units

Subsystem 4 of the presented Conceptual Model includes an overview and distribution of the units of analysis. This stage also largely determines the effectiveness of the system as certain units may match in meaning or have a specific character. In this case, the system, processing the accumulated units of analysis from the previous stage, determines the frequency of mention of the selected units, discarding a surplus of them that do not meet the set parameters and criteria. At the end, only the information that has a match in meaning, content or frequency of occurrence in a given text is extracted (Fig. 8).

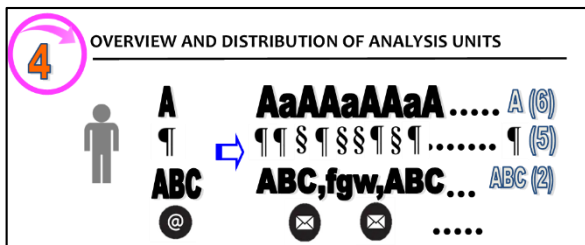


Fig. 8. Overview and Distribution of Analysis Units

The fifth stage, which is Subsystem 5 of the Conceptual Model structure, presents the direct counting of the results obtained from the previous stage in terms of the frequency of mention of units of analysis. Tables, computer programs and statistical calculations are most often used to successfully implement this stage of the analysis. The system tabulates the results obtained for each of the units of analysis (A; ¶; ABC; @) and performs an automatic reclassification by group of the number of these units (Fig. 9).

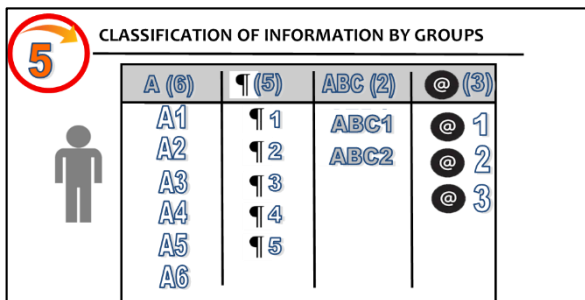


Fig. 9. Classification of Information by Groups

Subsystem 6 (Fig. 10) is also the sixth and final stage of the system operation, but not the last component of the presented Conceptual Model. Upon completion of the information assurance and analytical portions of the system operation, the resulting information product passes

through the presented filter for validation and recycling, which stands before the final output point of the overall Conceptual Model.

The purpose of the filter in the system is to scan and detect any information anomalies in the resulting information product. For this reason, the filter has sensors to identify content errors.

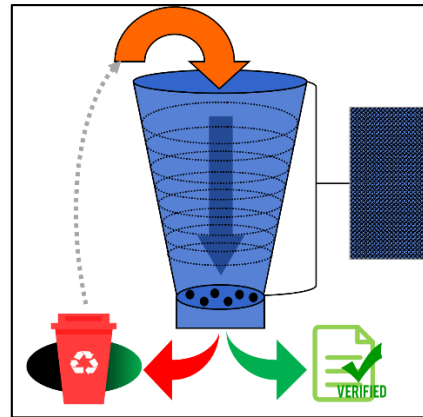


Fig. 10. Information Deviation Detection and Recycling Filter

The main criterion of the filter operation is based on the principle of authenticity (A = authenticity) of the information and reliability (R = reliability) of the source, borrowing for this purpose the functionality and principle of operation of the sensors for monitoring and detection of deviations.

In order to illustrate the filter operation mode, first of all, the information flow (iF) and its possible trajectory change under Average Deviation (Da) and Absolute Deviation (DA) are presented in Fig. 11.

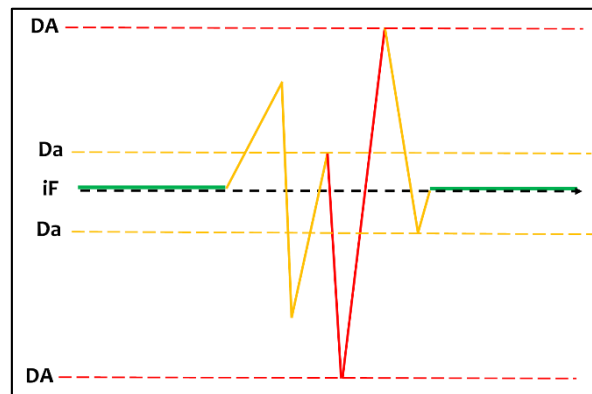


Fig. 11. Graphic Showing Deviations of the Information Flow - example

The information flow will remain on the rights then, when the structural or functional characteristics of the information flowing in it are not influenced by external or internal factors.

**Then:**

$$iF = f + s$$

In the case of mean information drift on the information flow, a partial manipulation has been exerted on the structural (s) or functional (f) characteristics of the information flow, as a consequence of which it will change

its trajectory. Examples of such manipulations are misinformation, propaganda, fake news, deception or online threats.

**Then:**

$$Da = A (f - s) - R (f + s)$$

**Or**

$$Da = - A (f - s) + R (f - s)$$

$$Da = A (f + s) + R (f - s)$$

Absolute deviation will be reported by the filter when the information does not meet the criterion in either the credibility or reliability part.

**Then:**

$$DA = - A (f - s) - R (f - s)$$

In the latter case, the information will be transferred to the database for recycling and storage. In this way, the automated system will use the accumulated information resource that does not meet the given criterion, using it to build a database with low credibility and reliability, which the system will then collate and not use. After the recycling mode, information that partially meets the criteria will be transferred for re-verification and final validation.

Information Validation (**iV**) will be executed by the system when the validity of the information and the reliability of the source have been confirmed and no structural or functional changes to the information flow have been identified:

$$iV = A (f + s) + R (f + s)$$

Recycling in the filter is the process of storing the information in the databases. In the case where the information does not meet the specified filter performance criterion, it will be stored in the blacklist database. In this way, by learning itself, the system will continuously add to this "list" and will not output the same content again.

Similarly, in the second case, the information that has gone through the non-verification process and comes out in the output as text will be stored in the verified database, which will be an additional guarantee of the quality of the source and will increase the value of the databases.

The seventh stage of the presented Conceptual Model consists in performing an expert interpretation of the results obtained due to the operation of the automated system for processing information from open sources and detecting information deviations.

In this stage, those characteristics of the generated result are identified and evaluated that allow general conclusions to be drawn, such as what is the meaning of the information obtained, whether its content is sufficient to draw conclusions and recommendations, whether the main problem has been solved or whether the causal relationships in it have only been partially inferred. It is no coincidence that the expert as a human factor in the automated system is at the centre of the triangle presented in Fig. 12.

His experience and knowledge determines the overall workflow of the system and, in particular, how the information will be processed so as to create opportunities

to perform interpretation on it. This point is also strongly tied to the element of subjectivity in information processing and analysis. This is due to the fact that the experience and knowledge of the expert, based on the value system, world view, cognitive and cultural orientation possessed by him, will break and modify to some extent parts of the flow of information units that pass through all stages of the system. The human factor, other than that of the author or creator of the information in its primary form, will affect the interpretation of the information.

Thus, the result at the end of the proposed Conceptual Model represents the analyst's interpretation, containing his experience and knowledge, combined with the results produced by the automated system. This is also a kind of process of generating new information and adding new knowledge in the domain for which the automated system is used.

As the starting point of the whole system, the distribution/consumption of the final result obtained in the form of a solution to the problem that arises at the input of the presented Conceptual Model is presented. The presented graphic shows the generated solution as new information generated, which comes out of the output and is transmitted to the end user (management unit, organization, institution, area).

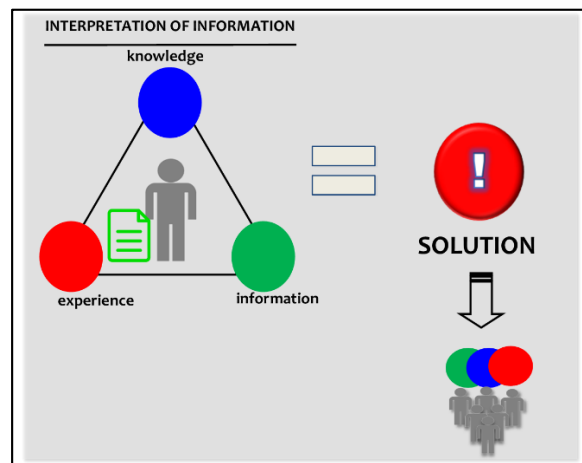


Fig. 12. Interpretation of Information

### CONCLUSIONS

The developed Conceptual Model (Fig. 13) is suitable for the selection of technical tools and software applications to build a unified information architecture that:

- reduces the impact of incomplete, ambiguous and erroneous data;
- assumes the availability of data at a higher level of abstraction;
- identifies missing information and the need for additional information.

The development of the Conceptual Model based on the JDL-model and borrowing the ideas embedded in human-machine interface methods aims to ensure that the information content of interest will be presented in a form that is suitable for user perception.

The Conceptual Model aims to represent the body of primary knowledge that has acquired a socially relevant status and, at the same time, to represent through specific structurally distinct relationships the knowledge and values that define information-analytic activity and the basic characteristics of information-processing systems.

One of the advantages and contributions of the Conceptual Model is the clear presentation of all stages of the system in a detailed and structured way, which could serve as a scientific basis for the development of an actual system.

The structural and functional characteristics of the Conceptual Model allow to make the connection between the different factors of influence in the implementation of the automated system operation.

The advantages of the proposed Conceptual Model provide:

- All significant knowledge classes that are explicitly described.
- Context-sensitive nature of knowledge extraction algorithms that is observable and controllable.
- Dynamic real-time information and data processing.
- Maintaining a Database Management System containing static declarative knowledge that can be logically divided into context sensitive and context insensitive components.
- Capabilities to introduce correlation algorithms for multilevel, non-standard processing to produce a self-learning algorithm of the analysis procedure.

The use of an automated system to process information from open sources and detect information biases is necessary in intelligence for several reasons:

1. Efficiency: the automated system allows processing large volumes of data and information faster and more efficiently than human operators. This allows information acquisition and analysis to become an extremely fast process, which is essential in operational work.
2. Precision. It can use algorithms and models that are more accurate and reliable to detect potential threats and deviations.
3. Objectivity. The automated system is unbiased and objective as it is based on predefined rules and algorithms.
4. Scope. This allows for wider coverage of the information field and detection of unexpected relationships and patterns.
5. Security. This helps to reduce the risk of false or malicious information spreading and provide greater security to the collected data.

All of these factors make an automated system necessary and valuable to intelligence in processing information from open sources and detecting information deviations.

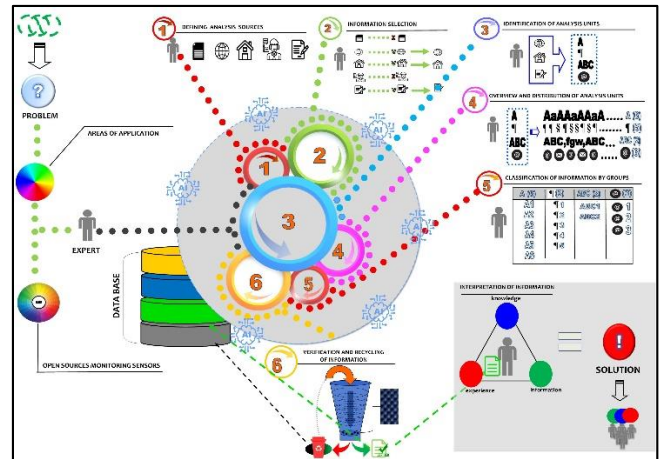


Fig. 13. Conceptual Model of an Automated System for Processing Information from Open Sources and Detecting Information Deviations

#### ACKNOWLEDGMENTS

This scientific paper 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] Semerdzhiev, Ts. Strategicheski informatsionni sistemi. Subekti na avtomatizatsiyata. Sofia: Softreyd, 2007, 273 s. [bulgarian language]
- [2] NATO Open Source Intelligence Handbook, November 2001. [Online] Available: <https://github.com/lawsecnet/OPSEC/blob/master/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf>. [Accessed: Feb. 20, 2024].
- [3] OSINT Handbook by Open Source Center, Romanian Intelligence Service, 2018. [Online]. Available: <https://bib.opensourceintelligence.biz/STORAGE/OSINT%20Handbook.pdf>. [Accessed: Feb. 20, 2024].
- [4] Thompson, J. R., R. Hopf-Weichel, and R. E. Geiselman. The Cognitive Bases of Intelligence Analysis, Arlington, VA: U.S. Army Intelligence and Threat Analysis Center Report No. R83-039C, 1984, pp. 2–9.
- [5] Ungureanu, Gabriel-Traian. Open Source Intelligence (OSINT). The Way Ahead. – In: Journal of Defense Resources Management, Vol. 12, Issue 1 (22)/2021, p. 179.
- [6] Williams, H., I. Blum. Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. RAND Corporation, California, 50 p.
- [7] Bielska, A., N. Kruz, Y. Baumgartner, V. Benetis. Open Source Intelligence Tools and Resources Handbook. Switzerland: I-Intelligence, 2020. 510 p.
- [8] Hirschheim, R., H. Klein, K. Lyytinen et al. Information Systems Development and Data Modeling, November 2011. [Online]. Available: <https://www.cambridge.org/core/books/information-systems-development-and-data-modeling/DE7DF31E05AB4F4BF579E7448167B715> [Accessed: Feb. 21, 2024].
- [9] Cambridge: Cambridge University Press, 1995. 303 p.
- [10] Yordanova, S. Informatsionni voyni. Informatsiyata – orazhieto na savremennia syvat. – V: Sbornik s dokladi ot Godishna universitetska nauchna konferentsia, 30 yuni – 1 yuli 2022, Veliko Tarnovo. Veliko Tarnovo: NVU „Vasil Levski“, 2022, s. 185–192. ISSN 1314-1937. [bulgarian language]
- [11] Kazakov, K. Protivodeystvie na zabluda v natsionalnata sigurnost. – V: Obshtestvoto na znaniето i humanizmat na XXI vek: XIX natsionalna nauchna konferentsia s mezhdunarodno uchastie Sofia, 1 noemvri 2021 g. Sofia: Za bukвите – O pismenehy, 2021, s. 438–444. [bulgarian language]

- [12] Kazakov, K. Strategicheskoye upravleniye na informatsionnyye uslugi v sigurnostta. Sofia: Softtreid, 2019. 232 s. [bulgarian language]
- [13] Kazakov, K. Falshivite novini kato instrument za manipulirane na obshtestvenoto mnenie. – V: Obshtestvoto na znaniye i humanizmat na XXI vek: XIX natsionalna nauchna konferentsia s mezhdunarodno uchastie Sofia, 1 noemvri 2021 g. Sofia: Za bukвите – O pismenehy, 2021, s. 438–444. [bulgarian language]
- [14] Yotova, R. Open Sources of Information. Collection, Classification And Processing. Sofia: Za bukвите – O pismeneh, 2023, 224 p. [bulgarian language]
- [15] Zahariev, A. Informatsionnata sigurnost i zashtita na informatsiyata. – V: Sbornik nauchni trudove ot Nauchna konferentsia „Problemi na informatsionnata sigurnost prez XXI vek“, Shumen, 2011. Shumen: Natsionalen voenen universitet „Vasil Levski“, 2011, s. 245-250. ISBN 978-954-9681-49-9. [bulgarian language]
- [16] Angelov, G. Arhitekturen podhod za opisaniye na protsesite v komunikatsionno-informatsionni sistemi na organizatsionno-upravlenski strukturi. – V: Obrazovanie, nauchni izsledvaniya i inovatsii, godina I, knizhka 3, 2023, s. 36-42. ISSN 2815-4630. [bulgarian language]
- [17] Boyanov, S. Energiynite resursi kato sredstvo za vliyanie v usloviyata na geopoliticheskoye protivopostavyane. Nyakoi aktualni sabitiya i proyavleniya, zasyagashti natsionalnata sigurnost. – V: Sigurnost i obrana. Aktualno sastoyanie, vazmozhnosti i perspektivi. Sofia: Za bukвите – O pismenehy, 2023, s. 380-390. ISBN 978-619-185-593-3. [bulgarian language]

# Methodology for Evaluation of Strategic Documents

**Zarko Zdravkov**

National Defense College "G. S. Rakovski"  
Sofia, Bulgaria  
z.zdravkov@rndc.bg

**Anelia Atipova**

National Defense College "G. S. Rakovski"  
Sofia, Bulgaria  
a.atipova@rndc.bg

**Abstract.** The nature of the strategic documents and the mechanisms for their updating require improvement of the strategic planning apparatus. Despite the existing actions in this direction, there is still no universal state standard and mature regulatory framework to harmonize and regulate the entire process in the Republic of Bulgaria. The report summarizes efforts to create a new toolkit bringing together proven practices in the subject area. A Methodology for the evaluation of strategic documents is presented, which offers a comprehensive and systematized approach to the evaluation of conformity according to the procedure of creation, structure, consistency, content and attainability.

**Keywords:** strategic planning; evaluation methodology; strategic document; national strategy.

## I. INTRODUCTION

As one of the main deficiencies of the existing strategic planning apparatus, the lack of a comprehensive approach to analysis and evaluation of national strategies can be pointed out.

The currently applied approach is expert evaluation, as the sequence, scope, criteria and depth of the research are not specified in advance, but are at the personal discretion and competence of the expert. As a result, expertises are obtained that can hardly be combined into a comprehensive assessment that examines the problem in the necessary scope and depth. The problem is deepened also due to the fact that in the process of evaluating strategies of such a rank, experts from different institutions with different areas of expertise are involved. This inevitably leads to distortions in the expert evaluations, as the questions that fall within the expert focus of the expert are overexposed, and those that are outside are ignored.

To overcome this shortcoming, the Methodology for the evaluation of strategic documents was developed, offering a comprehensive and systematized approach to evaluation, by summarizing formalized and strictly framed expert evaluations. The methodology includes a

formalization model that defines the purpose, scope and necessary tools of the research.

The final result of the analysis is a summary of assessments by experts applying the methodology independently of each other.

## II. MATERIALS AND METHODS

National strategies are considered within the national and union strategic frameworks, only in relation to higher-level strategic documents.

Methods relevant to the purposes of the analysis were used, such as content analysis, SWOT, PESTLE, Brainstorming, criteria analysis and risk analysis, not excluding, at the discretion of the experts, the application of others.

## III. RESULTS AND DISCUSSION

The Methodology for evaluation of strategic documents carries out evaluations in directions arising from the general conditions (the national environment) in which documents are being created and are functioning, as follows:

1. Compliance in terms of creation procedure.
2. Compliance in terms of structure and consistency.
3. Compliance in terms of content.
4. Achievability assessment.

The criteria for analysis in the directions are synthesized from the regulatory framework and the principles in the theory of strategic planning [1].

### A. Evaluation of compliance in terms of creation procedure of a strategic document

The evaluation of compliance in terms of creation procedure of a strategic document provides information on the integrity, actuality, legitimacy and degree of public acceptance of the strategic document. It is performed by setting values of the criteria shown in Table 1.

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8218>

© 2024 Zarko Zdravkov, Anelia Atipova. Published by Rezekne Academy of Technologies.  
This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)



TABLE 1 COMPLIANCE ASSESSMENT OF A STRATEGIC DOCUMENT ACCORDING TO THE CREATION PROCEDURE

№	Evaluation criteria by creation procedure	Performance level
1	Acceptance time relative to accepted senior documents	Yes/Partly/No
2	Acceptance time relative to the document's up-to-dateness	Yes/Partly/No
3	Authorities responsible for creating the document	Yes/Partly/No
4	Availability of public consultations on time	Yes/Partly/No
5	Existence of an evaluation cycle evidenced by reports on: <ul style="list-style-type: none"> <li>• Preliminary evaluation – performed at the document development stage.</li> <li>• Mid-term evaluation – performed at the stage of implementation of the strategic document and monitoring of activities.</li> <li>• Follow-up evaluation – is carried out at the stage of completion of the action of the strategic document.</li> </ul>	Yes/Partly/No
5.1	Preliminary assessment	Yes/Partly/No
5.2	Intermediate assessment	Yes/Partly/No
5.3	Follow-up assessment	Yes/Partly/No
6.	Publicity	Yes/Partly/No

The evaluation indicator is "Performance level" and indicates whether the relevant criterion is present and meets the requirements. Accepts values from a three-point ranking scale, with the following values:

- Fulfilled ("Yes") - the criterion is fulfilled in full;
- Partially fulfilled ("Partially") - the criterion is fulfilled with known limitations, which are briefly stated in free text;
- Unfulfilled ("No") – the criterion is not fulfilled.

**B. Evaluation of compliance in terms of structure**

The evaluation of compliance in terms of structure reveals the compliance of the evaluated strategy with the necessary structural elements (components) of this type of documents. The requirements for the structure of a strategic document adopted by the theory are shown in Table 2:

TABLE 2 EVALUATION OF STRATEGIC DOCUMENTS OF COMPLIANCE IN TERMS OF STRUCTURE

№	Structural elements of a strategy (components)	Fulfilled
1	Analysis of the current state	Yes/No
2	Vision for development	Yes/No
3	Strategic goals	Yes/No
4	Regional dimensions and projections	Yes/No
5	Activities and/or reforms to achieve strategic goals	Yes/No
6	Expected results of activities and/or reforms (indicators)	Yes/No
7	Financial framework for achieving the goals and results	Yes/No
8	Institutions responsible for implementation, monitoring and control	Yes/No

The structural elements of a national strategy may vary in name, while retaining their semantic value and are evaluated by an indicator: "Degree of implementation", with values "Fulfilled" and "Unfulfilled".

**C. Evaluation of compliance in terms of consistency**

A consistency assessment reveals the consistency, comprehensiveness, the presence of overstatement and contradictions in the development of the main ideas, following the content of the document. Document consistency is determined by cross-component analysis, with the components of the analysis being the structural elements of the document (Table 2). According to the logic of hierarchical structures, the analysis follows the development of the issues under consideration in the relationships between senior and junior components, assessing how the issues under consideration in the senior components are further developed in the junior ones.

Relationships between the components (structural elements of the document) subject to analysis are shown in Figure 1.



Fig. 1. Relations between document components.

To ease the research work, the relationships to be analyzed between the components of Figure 1 can be tabulated (Table 3).

TABLE 3 CROSS-COMPONENT ANALYSIS LINKS

Analyzed component	Assessment by:
1. Analysis of the current state	Output component
2. Development vision	1. Analysis of the current state
3. Strategic objectives	1. Analysis of the current state 2. Vision for development
4. Forecasts for changes in the region	1. Analysis of the current state 2. Vision for development 3. Strategic objectives
5. Activities and/or reforms to achieve the strategic goals	Strategic objectives
6. Expected results of the activities and/or reforms (indicators)	5. Activities and/or reforms to achieve strategic objectives
7. Financial framework for achieving the objectives and results of the strategy	5. Activities and/or reforms to achieve strategic objectives
8. Institutions responsible for implementation, monitoring and control	5. Activities and/or reforms to achieve strategic objectives

The questions addressed in the components contained in the column "Assessment by:" should be embedded in a

component from the column "Strategic document component" located on the same row (Table 3).

For the purposes of the cross-sectional analysis, each of the questions under consideration is taken as a base statement and an output prediction that is followed in the text. To facilitate visualization in the analysis, by means of a tabular representation, it is recommended that the links intercomponent connecting two elements of the structure of the strategic document through the base statements and the output forecasts be coded as follows:

$$BMC_{n,m} = \{CC_n, IC_m, BS_{a,(n,m)}, OP_{b,(n,n)}\} \quad (1)$$

where:  $n=m$  are the components numbers;

$a$  = number of a basic statement between the components  $n$  and  $m$ ;

$b$  = number of an output prediction between the components  $n$  and  $m$ ;

$CC_n$  – coding component;

$IC_m$  – interpretive component;

$BS_{a,(n,m)}$  – basic statement between the components  $n$  and  $m$ ;

$OP_{b,(n,n)}$  – output prediction between the components  $n$  and  $m$ .

In fact, a relation between two components is understood to mean the set of all output predicates and basic statements that are valid for those two components. Basic statements and output predictions linking the components of a strategic document relative to the links in Table 3 are shown in Table 4.

TABLE 4 BASIC STATEMENTS AND OUTPUT PREDICTIONS, CONNECTING THE COMPONENTS

		Interpretive components							
		C <sub>1</sub>	C <sub>2</sub>	C <sub>3</sub>	C <sub>4</sub>	C <sub>5</sub>	C <sub>6</sub>	C <sub>7</sub>	C <sub>8</sub>
Coding components	C <sub>1</sub>								
	C <sub>2</sub>	$BMK_{2,1}$							
	C <sub>3</sub>	$BMK_{3,1}$	$BMK_{3,2}$						
	C <sub>4</sub>	$BMK_{4,1}$	$BMK_{4,2}$	$BMK_{4,3}$					
	C <sub>5</sub>			$BMK_{5,3}$					
	C <sub>6</sub>					$BMK_{6,5}$			
	C <sub>7</sub>					$BMK_{7,5}$			
	C <sub>8</sub>					$BMK_{8,5}$			

The evaluation criteria when performing an inter-component analysis for consistency are: "Consistency", "Completeness" and "Contradiction", which provide information on the development, sufficiency and deviations in the identified basic statements and output predictions in the text. The criteria are measured on a rating scale, with "Consistency" and "Contradiction" entered as "Present" and "Absent," and the "Completeness" criterion is rated as "Incomplete," "Complete" and "Overexposed".

#### D. Evaluation of compliance of strategic documents in terms of content

The text of the document follows its structure, as in each component (structural element) the ideas implied in its name are further developed. Assessment of compliance

with the content of the strategic document is carried out through expert analyses, comparing the content of its components with reference information previously created by the expert in the Assessment Framework (Figure 2).

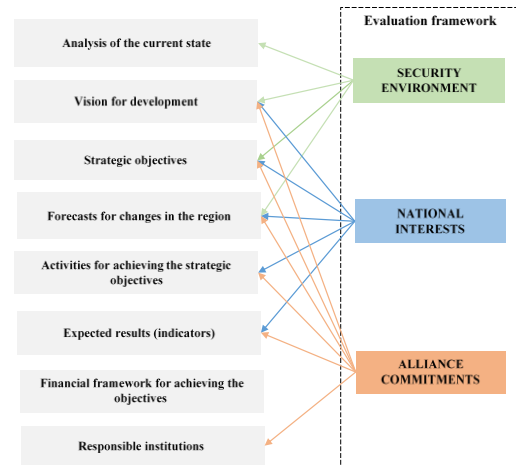


Fig. 2. Evaluation by content.

#### a. Evaluation framework

The framework for evaluating strategic documents defines the current state and covers the domains: "Security Environment", "National Interests" and "Union Commitments" (Figure 2).

The "Security Environment" domain is defined by internal and external factors and forces influencing national policies to achieve strategic goals and priorities. In the domain, the following parameters are uniquely defined to be matched with the information in the document:

- Parameter 1.1., "External factors in the security environment" – refers to the external factors (regional and global level) from which the main security threats arise.
- Parameter 1.2., "Internal factors in the security environment" - refers to the internal factors from which the main threats arise.

The "National Interests" domain is defined by higher-ranking documents, i.e. national strategies are analyzed against relevant national program documents, and sectoral strategies against relevant national strategies. Parameters to determine are :

- Parameter 2.1., "Long-term objectives" - refers to the framework of goals set in documents of a higher rank;
- Parameter 2.2., "Priorities" - refers to the prioritization made in documents of a higher rank;
- Parameter 2.3., "Starting points of the development vision" - refers to the development vision defined in documents of a higher rank.

These parameters reveal the degree of continuity and coordination between the goals, priorities and visions of the evaluated documents.

- Parameter 2.4., "Financial framework for implementation" - refers to the financial framework for the implementation of the strategic document defined in documents of a higher rank.

The parameter reveals the coherence of a financial framework to achieve the objectives.

The “Alliance Commitments” domain is defined against supranational alliance frameworks (UN, EU and NATO). The parameters to determine are:

- Parameter 3.1., "Fundamental principles of the organization/union" - refers to the fundamental principles of the organization/union;
- Parameter 3.2., "Main goals and priorities of the organization/union" - refers to the main goals and priorities of the organization/union;
- Parameter 3.3., "Main tasks of the organization/union" - refers to the main tasks of the organization/union;
- Parameter 3.4., "Mechanisms for sustainability" - refers to the persistent mechanisms for achieving the goals set by the organization/union;
- Parameter 3.5., "Mechanisms for continuity" - refers to the continuity determined for the member state in the mechanisms for implementing the shared functions of the organization/union.

**E. Evaluation of content**

Evaluation of the content of the strategy document is carried out by matching the content of its components with the domains in the evaluation framework (Figure 2). The components of the strategy document are reviewed sequentially to ascertain the availability of information and its alignment with each of the domains in the assessment framework.

When determining the availability of information, it is filled as it is shown in Table 5.

TABLE 5 EVALUATION OF A STRATEGIC DOCUMENT COMPLIANCE IN TERMS OF CONTENT

Strategic document component	Domains in the evaluation framework		
	Security environment	National interests	Alliance commitments
1. Analysis of the current state	Yes/No		
2. Vision for development	Yes/No	Yes/No	Yes/No
3. Strategic objectives	Yes/No	Yes/No	Yes/No
4. Forecasts for changes in the region	Yes/No	Yes/No	Yes/No
5. Activities and/or reforms to achieve the strategic goals		Yes/No	Yes/No
6. Expected results of the activities and/or reforms (indicators)		Yes/No	Yes/No
7. Financial framework for achieving the objectives and results of the strategy			
8. Institutions responsible for implementation, monitoring and control			Yes/No

If information is not found, the value "No" is filled in and a specific weakness/deficiency of the document is registered.

With a value of "Yes", a subsequent expert evaluation is performed for compliance according to the parameters of the specific domain. The evaluation criteria are as follows:

Criterion 1 "Relevance" - evaluates the current validity of the components, relative to parameters in the evaluation domain;

Criterion 2 "Adequacy" - assesses the accuracy of reflection in the components of parameters from the assessment domain;

Criterion 3 "Completeness" - evaluates the degree of reflection (description) of the entered parameters, relative to the assessment domain.

The criteria are evaluated on a rating scale that has the following values:

- Available – full presence of the criterion is registered;
- Partial – partial presence of the criterion is registered;
- Missing – the presence of the criterion is not registered.

**F. Achievability assessment**

The assessment of the achievability of the strategic objectives includes the identification, registration and systematic evaluation of the risks for the implementation of the strategies [5], by means of risk analysis methods [6]. The main types of strategic risk before the implementation of the state policy laid down in the strategy are: economic, technological, socio-cultural risks, risks related to institutional capacity and political-military risks. Risk matrices [7] are used to assess the risk, which indicate its probability and the severity of the consequences.

To track the risks, they are filled in a risk register table (Table 6).

TABLE 6 EXAMPLE TABLE FOR REGISTERING RISKS

№	Name of the risk	Description	Level of probability			Level of impact			Overall assessment		
			High	Average	Low	High	Average	Low	High	Average	Low
Economic risks											
1											
2											
Technological risks											
1											
2											
Socio-cultural risks											
1											
2											
Institutional risks											
1											
2											
Political-military risks											
1											
2											

**G. Recommendations for the development of national strategies**

The recommendations for the development of national strategies are the final part of the Methodology and include a reasoned statement of the opinion of the analysts who participated in the evaluation of the strategic documents. They refer to adjusting the objectives, the activities to achieve them, as well as the risk management activities.

When the risks to the objectives of the national strategy are assessed, a matrix for objectives achievement, which is essentially an extended risk-register [8] and includes the components: objective, activities to achieve the objective, expected result, indicators for reporting progress, deadlines, identified risk to the objective and risk level, risk mitigation activities, residual risk level and responsible risk management institutions.

The recommendations do not deviate from the standards for drafting a strategic document, described in the Methodology for Strategic Planning in the Republic of Bulgaria [9] and the Draft Law on Strategic Planning in the Republic of Bulgaria [10].

#### CONCLUSIONS

A methodology for the evaluation of strategic documents is proposed, which offers a comprehensive and systematized approach to the evaluation of compliance in terms of creation procedure, structure, consistency, content and attainability.

According to the methodology, formalized and strictly framed independent expert evaluations of the same type are carried out, as the final evaluation of each aspect is the generalized prevailing hypotheses. A report is prepared, in the Bottom Line Up Format [11], which has the following components: key points, introduction, statement, conclusion, references and appendices.

Introducing a strict model of formalization, the methodology gives the consistency of the analysis, defines the evaluation criteria for each direction and recommends the use of popular and proven tools for analysis. Placing in a narrow framework the creation of expert assessments leads to a decrease in subjectivity, i.e. an increase in objectivity. The final result is a report where the expert assessments are summarized according to the prevailing opinions of the experts, which is a prerequisite for high legitimacy of the results.

The Methodology offers an invariant approach, which makes it suitable for evaluation in the process of strategic planning in all socio-economic spheres.

The Methodology has been verified, having been applied in the assessment of the National Security Strategy of the Republic of Bulgaria. The results are published in a report entitled "Assessment of the Actualized national security strategy of the Republic of Bulgaria" [12] presented on the "International conference on advanced research and technology for defence - ARTDEF 2023", of the Bulgarian Defense Institute "Professor Tsvetan Lazarov". At the moment, the methodology is being applied to evaluate the Project of the National Defense Strategy of the Republic of Bulgaria, and the results are yet to be published.

#### 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".

#### REFERENCES

- [1] COMMISSION STAFF WORKING DOCUMENT Performance, monitoring and evaluation of the European Regional Development Fund, the Cohesion Fund and the Just Transition Fund in 2021-2027, [https://ec.europa.eu/regional\\_policy/sources/docgener/evaluation/pdf/performance2127/performance2127\\_sw\\_d.pdf](https://ec.europa.eu/regional_policy/sources/docgener/evaluation/pdf/performance2127/performance2127_sw_d.pdf) [Accessed March 13, 2022].
- [2] UN Sustainable Development Goals, <https://strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=1330> [Accessed March 15, 2022].
- [3] European Strategy for Sustainable Development, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52001DC0264> [Accessed March 13, 2022].
- [4] Strategic Concept of NATO 2022, <https://www.nato.int/strategic-concept/index.html> [Accessed August 24, 2022].
- [5] ISO 31000:2018, International Risk Management Standard [Accessed April 16, 2022].
- [6] IEC 31010:2019 Risk management. Risk assessment techniques
- [7] Julian Talbot, "What's right with risk matrices?", July 9, 2017, [What's right with risk matrices? \(juliantalbot.com\)](http://What's%20right%20with%20risk%20matrices%20(juliantalbot.com)) [Accessed February 23, 2022].
- [8] Team Asana, What is a risk register: a project manager's guide (and example), December 5th, 2022, [Risk Register: A Project Manager's Guide with Examples \[2023\]](http://Risk%20Register:%20A%20Project%20Manager's%20Guide%20with%20Examples%20[2023]) [Accessed February 23, 2022].
- [9] Methodology for strategic planning in the Republic of Bulgaria, <https://www.strategy.bg/Publications/View.aspx?Id=90> [Accessed April 17, 2022].
- [10] Draft Law on Strategic Planning in the Republic of Bulgaria [Accessed April 17, 2022].
- [11] BLUF: The Military Standard That Can Make Your Writing More Powerful, <https://www.animalz.co/blog/bottom-line-up-front/> [Accessed April 18, 2022].
- [12] Z. Zdravkov, A. Atipova, S. Stoykov, Assessment of the actualized national security strategy of the Republic of Bulgaria, International Conference on Advanced Research and Technology for defence - ARTDEF 2023, ISSN 2815-2581

# *The Applicability of the EU Data Protection Rules in the Area of National Security 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](mailto:m.zahariev@unibit.bg)

**Abstract.** The key acts shaping the EU data protection legal regime – the General Data Protection Regulation 2016/679 (GDPR) and the Law Enforcement Directive 2016/680 (LED) – explicitly stipulate that they do not apply in areas which fall outside the scope of EU law, such as activities concerning national security (recital 16 and 14 respectively). At the same time, Bulgarian legislation gives a very broad definition of “national security” as a dynamic state of society and the state in which values such as the territorial integrity, sovereignty and the constitutionally established order of the country are protected, and where the democratic functioning of institutions and the fundamental rights and freedoms of citizens are guaranteed. As a result, a variety of competent authorities contribute daily to the protection of these values such as the leading authorities from the legislative and executive power, the president, the law enforcement agencies, the courts, the various regulators, etc. A lot of the data processing activities of these authorities conducted while exercising their powers actually do fall into the scope of the GDPR and the LED and at the same time serve the protection of the national security. To that end, a strict dividing line between national security and other activities of these bodies often cannot be drawn. The present paper argues that the GDPR and the LED should apply to a lot of the activities contributing to the protection of national security which will also be an additional safeguard for the fundamental rights and interests of the individuals and increase the accountability of the competent authorities.

**Keywords:** *GDPR, LED, national security, data protection, competent authorities.*

## I. INTRODUCTION

The present study aims to explore the notion of national security from the perspective of the legislation of Republic of Bulgaria – a Member State of the EU – in the context of personal data processing activities. The goal of this analysis

is to prove that the concept of national security is so broad that a strict dividing line between national security and other activities of the competent authorities and bodies whose powers serve the protection of the national security often cannot be drawn. Ultimately, the present paper argues that the EU laws on data protection should actually apply to a lot of the activities contributing to the protection of national security which will also be an additional safeguard for the fundamental rights and interests of the individuals and increase the accountability of the competent authorities.

The background of the researched problem can be summarized as follows: the key acts shaping the EU data protection legal landscape – the General Data Protection Regulation 2016/679 (GDPR) [1] and the Law Enforcement Directive 2016/680 (LED) [2] – explicitly stipulate that they do *not* apply in areas which fall outside the scope of EU law, such as activities concerning national security (recital 16 and 14 respectively). This is also reaffirmed by the Treaty on the European Union (TEU) [3] which stipulates that national security remains the sole responsibility of each Member State (Art. 4(2) of the TEU). At the same time, EU law lacks a specific definition for “national security”, although the Court of Justice of the EU (CJEU) in its practice has shed some light on this concept. In particular, in its Judgement on Joined Cases C 511/18, C 512/18 and Case C 520/18 CJEU has interpreted the cited Art. 4(2) of the TEU, highlighting that the said responsibility of the Member States to ensure their national security “*corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly*

Print ISSN 1691-5402  
Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8234>

© 2024 Martin Zahariev. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

threatening society, the population or the State itself, such as terrorist activities” [4]. Evident from the above, what constitutes national security and which activities fall or do not fall therein should be defined in the national legislation of each Member State. In any case, these activities should meet the following cumulative criteria (i) serve the essential state functions and the fundamental interests of the society and (ii) prevent and sanction activities threatening fundamental values such as constitutional, political, economic or social structures, the society, the population or the state itself. As the focus of the present study is the Republic of Bulgaria, the next section is devoted to clarifying this concept from Bulgarian legal perspective.

## II. METHODOLOGY OF THE STUDY

The results of the present study were obtained after applying scientific methods such as:

- *Documentary method* – consisting in analyzing and synthesizing information about the definition of national security from various documentary sources – e.g. from the primary and secondary EU law, from Bulgarian national legislation and from other publicly available (including online) sources, as well as in the systematization and summarization of this information.
- *Historical method* – this method is used to track the dynamics of the Bulgarian data protection legislation before and after the adoption of the GDPR and the LED and the transposition of the latter in the national legislation and the changes in the legal concept of national security.
- *Comparative analysis* – this method consists of comparing the common and the different between separate phenomena. In this report, this method is necessary to prove that often certain activities of the competent authorities cannot be classified in a straightforward manner whether they fall into one or another data protection regime.
- *Case study* – this method is used to illustrate how certain activities that fall into the EU data protection regime can contribute to protecting national security.
- *De lege ferenda* – this specific scientific method is used in the law science to propose future amendments in the legislation.

## III. RESULTS

### A. *The Concept of National Security under Bulgarian Law*

The Bulgarian law contains a definition of “national security” in the Management and Operation of the National Security Protection System Act (MONSPSA) [5] which reads as follows: “National security is a dynamic state of society and the state, in which the territorial integrity, sovereignty and constitutionally established order of the country are protected, when the democratic functioning of the institutions and the basic rights and freedoms of the

citizens are guaranteed, as a result of which the nation preserves and increases its well-being and develops, as well as when the country successfully defends its national interests and realizes its national priorities” (Art. 4(2)). The Bulgarian legal scholars have emphasized that the term “national security” in the past has been defined in various legal acts such as the Protection of Classified Information Act [6] and the State Agency National Security Act [7] which reveal “differences in some understandings”, but “through the law (the MONSPSA – note of the author) a uniform definition of this concept has already been adopted” [8]. This is also reaffirmed by the Updated Strategy for National Security of the Republic of Bulgaria (the Strategy), which provides that with the adoption of the MONSPSA, “a uniform legal definition of the concept of national security has been adopted” (para. 6) [9]. In addition, the Strategy acknowledges that “the final product and the real meaning of the concept of “national security” is the guarantee of human security and the protection of the freedom and dignity of the citizen, as well as the protection of sovereignty, territorial integrity and the protection of the state border” (para. 9) [9].

At the same time, various scholars have examined the notion of national security both in general [10], [11], [12] as well as in its different manifestation forms in areas such as (i) the migrant smuggling [13]; (ii) the importance of natural resources for the national security [14]; (iii) the policy of countries neighboring to Bulgaria such as Republic Turkey [15]; (iv) the internal activities of some public bodies and their importance for the national security [16]; (v) the demographic problems [17]; (vi) the possibility of the national security to be considered as part of the overriding mandatory provisions in private international law [18].

These nuances are important, because they outline different directions in which competent authorities by exercising their powers can ultimately contribute to safeguarding the national security.

### B. *Case Study*

The present part is devoted to provision of several practical examples of activities both falling into the scope of the EU data protection laws and protecting national security:

**Example:** A foreign national – e.g. an undercover agent – is instructed by his government to hack key information systems of the Republic of Bulgaria such as the electronic records of the National Revenue Agency and the Ministry of Interior. He should instal malware therein which could result in unlawful extraction, alteration and/or loss of the contained data, including personal data of hundreds of thousands of Bulgarian citizens. The purpose is to create fear and uncertainty among the society, and ultimately – to destabilise the established state order by compromising the activity of important state authorities that are vital for the functioning of the economy and internal security.

In any case, this is an unlawful activity threatening key elements of the national security enlisted above such as (i) the constitutionally established order, (ii) the democratic functioning of the institutions and (iii) the basic rights and freedoms of the citizens. At the same time, at least the following authorities may need to be involved to

investigate and sanction the matter and to protect the rights of the affected citizens (and by exercising their powers, to conduct related data processing activities):

- Ministry of Interior, the State Agency “National Security” and competent investigators – to investigate the crime;
- State Agency “Technical Operations” – to apply special intelligence means, in case such are needed for revealing the perpetrator(s);
- Prosecutor – to supervise the investigation during the pre-trial phase of the criminal proceedings, to decide when there are sufficient evidence to press charges, which person(s) to be charged and for what type of crime(s), to maintain the charge before the court during the trial phase of the criminal proceedings;
- Criminal court – to consider the case, and if the charges are proven – to impose criminal liability;
- Competent cybersecurity authorities – to the extent that the crime constitutes severe cybersecurity accident;
- Ministry of Electronic Government, Ministry of Defence and Ministry of Finance – to cooperate to the extent they are competent – with the above authorities, as the crime could affect the spheres where they are competent;
- State Commission for Protection of the Information – if classified information is affected;
- The President of the Republic, the Council of Ministers and the National Assembly – as key state authorities, may need to take appropriate actions to ensure the stability of the state and the society – depending on their powers;
- Commission for Personal Data Protection – where the affected citizens may file complaints to seek protection of their data protection rights and which – as data protection supervisory authority – should be competent to evaluate the data protection implications of the crime, as it constitutes a data breach under the GDPR (Art. 4, item 12 and Art. 33-34) and the LED (Art. 3, item 11 and Art. 30-31);
- Administrative Courts – where the affected citizens may file claims for monetary compensation of the damages suffered by the data breach.

### C. Key Takeaways from the Case Study

In the light of the case study, two possible approaches exist when dealing with data protection in the context of national security:

A *formalistic (restrictive) approach* which automatically excludes any activity related to national security from the scope of the data protection rules. This approach is supported by the quoted provisions of the TEU, the GDPR and the LED. Also, Bulgarian Personal Data

Protection Act (PDPA) contains the restrictive rule that it does *not* apply to the processing of personal data for the purposes of the country’s defense and national security, *unless* a special law provides otherwise (Art. 1(5)) [19].

A *non-formalistic (realistic) approach* – a more balanced approach which aims to acknowledge that the notion of national security and the related activities are not black and white. This approach demonstrates that variety of data processing activities conducted by the competent state authorities when exercising their powers contribute on daily basis to the protection of national security and that the latter should not be limited solely to intelligence and counterintelligence activities. Of course, in the last two scenarios, the data protection rules shall apply with numerous and reasonable limitations. But it would be contrary to sense and the spirit of both the definition of national security and the EU data protection laws to generally and indiscriminately deny the application of the data protection rules in contexts such as the above presented in the case study. The latter, in particular the GDPR, provide for enhanced data subject’s rights (the GDPR extended existing data protection rights and added the new right of data portability [20]) and increased accountability of the data controllers (such as the public authorities). The last requirement according to the legal doctrine is related to the new philosophy of the GDPR and requires proactive approach from the data controllers with regard to the data processing activities [21]. Such rules in any case serve as an additional security for the lawfulness of the competent authorities’ activities. Also, if the formalistic approach is followed, this would deny the affected citizens from the possible tools for redress granted by the data protection rules (complaint, damage claim, etc.) which is hardly compatible with the element of national security guaranteeing the basic rights and freedoms of the citizens.

The non-formalistic approach is also supported by several arguments: First, the fact that the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties falls within the scope of EU data protection law, namely the LED. The majority of the activities enlisted in the case study actually can be classified as one or more of the above concepts, so the related data processing should be subject to the rules of the LED. Second, there are other activities that are borderline, i.e. that could simultaneously fall into different data protection regimes or at least where a strict borderline cannot be drawn – examples of such activity is the border control where sometimes it is very difficult to distinguish when a given processing operation related thereto is carried out for the purpose of combating crime and falls under the regime of LED when it is purely administrative by its nature and as such falls under the general regime of GDPR. As some authors have rightly pointed out, this often leads to an excessively broad interpretation of the LED, thereby undermining the application of the GDPR, and they point to border control, migration and asylum issues in many Member States as a specific example [22]. Third, some authors when analyzing the figure of data protection officer (DPO) have emphasized that the data controller does not appoint a DPO for each different processing purpose which means that the controller will be supported by one DPO (alone or with a team) for all processing purposes [23]. This

shows that even if the formalistic approach is followed and certain activities are defined as “strictly” national security-related, at least certain other data protection activities of public authorities with powers ultimately safeguarding the national security (such as the law enforcement agencies, courts, prosecution etc.) would still be subject to the GDPR and the LED.

Finally, it should be noted that recently Bulgarian PDPA has *diminished* the level of protection of individuals, as it reversed its approach towards data processing activities in the context of national security and law enforcement. In the past, before the amendments in PDPA from 2019 were made to align the PDPA with the GDPR and to transpose the LED, the PDPA stated that unless otherwise provided in a special law, the PDPA *also applied* to the processing of personal data for the purposes of: 1. the defense of the country; 2. national security; 3. the protection of public order and the fight against crime; 4. criminal proceedings; 5. the execution of punishments (Art. 1(5) of the PDPA – redaction before February 2019). As explained above, the current version of Art. 1(5) of the PDPA reads quite the opposite – the PDPA does *not* apply in these areas, unless otherwise provided for by specific law.

*De lege ferenda* it could be recommended that the old wording of the provision before the amendments of February 2019 is reinstated. This will ensure that the competent authorities adhere to the high standards of the GDPR and the LED when processing personal data and will ensure that the citizens (data subjects) whose personal data is processed by the said authorities when exercising their powers enjoy the enhanced level of protection granted by the said acts. This will also be in line with the historical traditions of the local data protection legislation, which, as already mentioned, used to apply to these spheres as well. In addition, as each Member State is solely responsible for its national security (as explained by the TEU and the CJEU), then every Member State is free to determine what data protection standards to apply to the competent authorities in these areas and the decision to subdue them to the rules under the PDPA transposing the LED for data processing in criminal and punishment context (a term introduced by some scholars to encompass the detailed enlisting in LED: prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties [23]) would not violate any EU laws.

#### CONCLUSION

In conclusion, the statement that in variety of scenarios a strict borderline between activities safeguarding the national security and the EU data protection laws cannot be made, seems justified. The criminal and punishment activities of the competent authorities when combating crime, the activities of the regulators when handling complaints and signals of the citizens, the activities of the courts when exercising their judicial powers are only minor examples of data processing activities subject to EU laws that contribute to the protection of national security. Ultimately, such an approach would be in line with the rule of law and the aim to ensure an additional protection for the fundamental rights and interests of the individuals and enhanced accountability of the competent authorities.

#### REFERENCES

- [1] Official Journal of EU, L 119, 4.5.2016, p. 1–88. Available: EUR-lex, <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [Accessed February 14, 2024].
- [2] Official Journal of EU, L 119, 4.5.2016, p. 89–131. Available: EUR-lex, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680> [Accessed February 14, 2024].
- [3] Official Journal of EU, C 202, 07.06.2016, p. 13–46. Available: EUR-lex, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12016ME/TXT> [Accessed February 14, 2024].
- [4] CJEU, Judgement on Joined Cases C 511/18, C 512/18 and Case C 520/18, para. 135, Available: Curia, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1579363> [Accessed February 14, 2024].
- [5] Promulgated in State Gazette, Issue 61 of 11.08.2015; last supplemented issue 15 of 22.02.2022 г., in force as of 22.02.2022.
- [6] Promulgated in State Gazette, Issue 45 of 30.04.2002; last amended and supplemented issue 84 of 06.10.2023, in force as of 06.10.2023.
- [7] Promulgated in State Gazette, Issue 79 of 13.10.2015, in force as of 01.11.2015; last amended issue 84 of 06.10.2023, in force as of 06.10.2023.
- [8] P. Bogdanov. Basics of the national security of the USA and the Republic of Bulgaria. Collection Knowledge Society and 21st Century Humanism The 20th International Scientific Conference Sofia, 1st November 2022. Sofia: Za bukвите – O pismeneh, 2022, p. 423–435. ISSN: 2683-0094.
- [9] Adopted via a decision of the National Assembly from or 14.03.2018, Promulgated in State Gazette, Issue 26 of 23.03.2018.
- [10] E. Manev. Global, Regional and National Security. Sofia: Softtrade, 2012, p. 382-486, ISBN: 978-954-334-141-2.
- [11] P. Bogdanov. Comparison of the National Security Systems of the USA and the Republic of Bulgaria. Collection of reports from the National Scientific Conference with international participation, held on April 21, 2023 at the University of Library Studies and Information Technologies “Security and Defense. Current Status, Opportunities and Perspectives“, Sofia: Za bukвите – O pismeneh, 2023, p. 72 – 85, ISBN: 978-619-185-593-3.
- [12] G. Angelov. Statehood and National Security. Sofia: Military publishing house, 2022, p. 54-74, ISBN: 978-954-509-581-8.
- [13] J. Deliversky. Migrants Smuggling as a Threat for the Economic, Social and National Security. Collection of reports from the Sixth National Conference with international participation MHANS, BAS, May 29 and 30, 2017, p. 221-226, ISSN: 1313-8308.
- [14] V. Lazarov. National Security Challenges in Relation to Resources. Collection Knowledge Society and 21st Century Humanism The 17th International Scientific Conference Sofia, 1st November 2019. Sofia: Za bukвите – O pismeneh, 2019, p. 625-632, ISSN: 2683-0094.
- [15] P. Teodosiev. Turkey’s Politics in Regional Conflicts – a Factor for the Threats and Risks to Bulgaria’s National Security. Collection of reports from the National Scientific Conference with international participation, held on April 21, 2023 at the University of Library Studies and Information Technologies “Security and Defense. Current Status, Opportunities and Perspectives“, Sofia: Za bukвите – O pismeneh, 2023, p. 387 – 396, ISBN: 978-619-185-593-3.
- [16] P. Teodosiev. Activity of the “Dossiers Commission“ and its Impact on the National Security of the Republic of Bulgaria. Collection Academic Partnerships in the Field of National Security - Shumen: “Konstantin Preslavsky” Univ., Assoc. Sci. and Appl. Research, 2022, p. 137 – 143, ISBN: 978-619-201-571-8.
- [17] M. Neykova, I. Prodanova. The Demographic Problem - a Threat to National Security. Juridical Collection of Bourgas Free University, vol. XXIV, 2017, p.11-18, Available: [https://www.bfu.bg/uploads/pages/jur\\_sbornik\\_20171.pdf](https://www.bfu.bg/uploads/pages/jur_sbornik_20171.pdf) [Accessed February 14, 2024], ISSN: 1311-3771.
- [18] Ts. Dimitrova. Hardship and Force Majeure in Private Law Relations with an International Element. The Question of Applicable Law. Sofia: Norma Magazine, Issue 1-2/2021, p. 60, ISSN: 1314-5126 (print).
- [19] Promulgated in State Gazette, Issue 1 of 04.01.2002, in force as of 01.01.2002; last amended issue 84 of 06.10.2023, in force as of 06.10.2023.



- [20] S. Dibble. *GDPR For Dummies*. Hoboken, New Jersey: John Wiley&Sons, Inc., 2020, p. 32. ISBN: 978-1-119-54609-2. Publishing and Bloomsbury Publishing Plc., 2022, p. 110-111, ISBN ePDF: 978-1-50995-965-5.
- [21] D. Toshkova-Nikolova and N. Feti, *Personal Data Protection*. Sofia: IK Trud I Pravo, 2019 p. 101, ISBN: 978-954-608-263-3.
- [22] T. Quintel. *Data Protection, Migration and Border Control: The GDPR, the Law Enforcement Directive and Beyond*. Oxford: Hart
- [23] N. Feti and D. Toshkova-Nikolova, *Application of the Personal Data Protection: Methodics, Recommendations and Practical Steps*. Sofia: IK Trud I Pravo, 2020 p. 505-506; 484-485, ISBN: 978-954-608-279-4.

# Study of the Operation, Maintenance, and Repair System of the Bulgarian Armed Forces

Ivan Malamov

Vasil Levski National Military University

Veliko Tarnovo, Bulgaria

ivan\_malamov@abv.bg

**Abstract.** Support of armaments and equipment is an integral part of the overall system for logistical support of the armed forces, which in turn represents a complex set of elements and interrelationships implementing the logistical functions to meet the emerging needs of the army and the fulfillment of the intended missions, goals and tasks. The main elements in this system are the management bodies and forces for the implementation of maintenance and repair activities, and the qualification and training of the latter is of essential importance for the timely restoration of damaged samples of armaments and equipment in the conditions of time deficit. The paper aims to examine the state of the operation, maintenance and repair system in the Armed Forces of the Republic of Bulgaria. Based on an empirical study with the armaments and equipment maintenance and repair specialists at different hierarchical levels, main problems arise from the supply of material resources for service and repair and the chain of their supply, the training and education of technical personnel and unclear allocation of responsibilities and activities regarding maintenance and repair.

**Keywords:** maintenance, repair, system, armed forces

## I. INTRODUCTION

In the modern world, maintenance and repair of equipment are an integral part of its operation and life cycle. It would be hard to imagine the world without service centers, workshops and factories to ensure the unhindered use of technology. However, this fact is not a given, but behind it lies long-term efforts and hard work of the people involved in the design, development, and maintenance of these technical means. In military conditions, technology is just as widespread as in the civilian sphere, and historical facts indicate that the latest technologies and inventions enter the military sphere first, and then the civilian sphere. This imposes the requirement for the existence of a well-functioning system for maintenance and repair of the weapons and equipment used, which would guarantee their unimpeded and reliable use in any environmental conditions.

According to the Doctrine for Logistics, "The system for logistic support of the armed forces is a set of management bodies, forces and means for carrying out the activities of providing the troops, connected in a single network of interconnections." [2], and the overall logistic support is carried out through a unified and coordinated implementation of the logistics functions. If each of the logistics functions is considered as an element of the logistics system, then viewed through the prism of the systematic approach, the influence of each element of the system would lead to a change in the overall state of the system. For instance, if we look at operation, maintenance and repair and the influence of other logistics functions on this element we could identify the main variables that affect this functional area. The aim of the present study is to establish the main motives (factors) for choosing the officer profession and present their importance and interconnectedness.

The study aims to confirm or disprove previously identified problems in scientific studies [3] and/or discover existing problems in the state of the operation, maintenance, and repair system.

## II. MATERIALS AND METHODS

The study of the operation, maintenance and repair system is based on a methodology developed specifically for the needs of the present study, based on data collection through a survey. The object of the research are three main target groups (categories) of military personnel from the Bulgarian Armed Forces. The three main categories are as follows:

- enlisted/civilian maintenance personnel;
- non-commissioned officers (NCOs);
- commissioned officers.

The scope of the research is the number of respondents by category:

- enlisted/civilian maintenance personnel – 241;

Print ISSN 1691-5402

Online ISSN 2256-070X

<https://doi.org/10.17770/etr2024vol4.8248>

© 2024 Ivan Malamov. Published by Rezekne Academy of Technologies.

This is an open access article under the [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

- NCOs – 188;
- officers – 104;

To achieve the objectives of the empirical study, three types of questionnaires were developed, with identical and specific questions for each surveyed category. They include two main parts: the first part - passport and the second part - questions structured by groups to reflect the opinion of the interviewed persons.

The passport part includes general information about the respondents.

In the second part, respondents have to answer structured questions and the answers could be given in the form of a Likert scale.

The scale contains five grades as follows: 1 – very low; 2 – low; 3 – medium; 4 – relatively high; 5 – very high.

### III.RESULTS AND DISCUSSION

The analysis of the results of the conducted survey is presented in individual or a group of questions from the survey card, taking into consideration the opinion of each of the categories.

Question 1 of the survey is identical for the enlisted/civilian personnel and NCOs and is identical with Question 2 of the commissioned officers survey, reading as follows:

"To what extent do you think the supply of material resources directly affects the quality and timely maintenance and repair of weapons and equipment (W & E)?"

The results for Question 1 are shown in fig.1.1, fig.1.2 and fig.1.3, with their analysis showing that a majority of about 59% of enlisted/civilian personnel and NCOs and 83% of the officers rate fairly high and very high the key role of material supply for the quality and timely maintenance and repair of W & E.

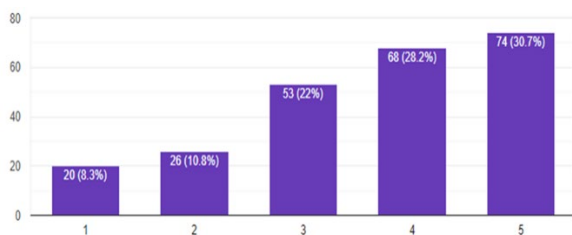


Fig. 1.1. Responses to Question 1 of the enlisted/civilian maintenance personnel.

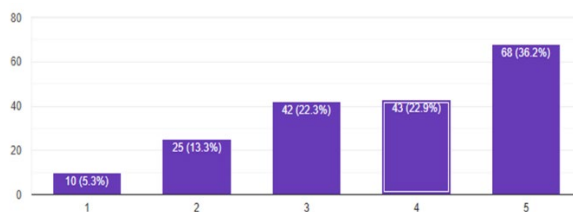


Fig. 1.2. Responses to Question 1 of the NCOs survey.

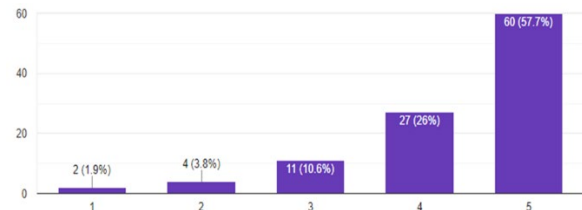


Fig. 1.3. Responses to Question 1 of the enlisted/civilian maintenance personnel.

Question 1 of the officers survey, specific to the interviewed category, is formulated as follows:

"To what extent do you think the other logistics functional areas influence the Operation, Maintenance and Repair functional area?"

This question is structured into eight sub-points containing the remaining eight functional areas of logistics and shows their interrelationship with operation, maintenance, and repair as part of the logistics system (Fig. 2). In this way, the respondents are given the opportunity to indicate what, in their opinion, is the degree of connectivity between the functional areas of logistics with operation, maintenance and repair.

The analysis of the results on this question shows that the officers indicate that the functional area Material Resource Supply plays the most significant role in performing maintenance and repair, followed by Movement and Transportation, Logistics Information Management and Providing Military Infrastructure.

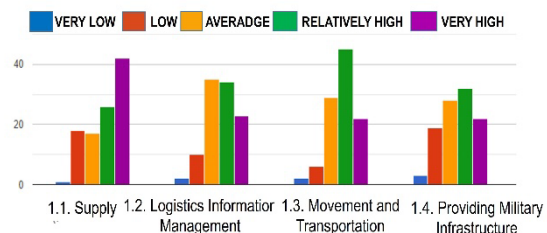


Fig. 2 Responses to Question 1 of the commissioned officers survey

Questions 2, 3, 4, and 5 of the enlisted/ civilian maintenance personnel and NCOs surveys are identical and match almost completely Questions 3, 4, 5, and 6 of the commissioned officers survey. They require the opinion of the respondents regarding stock availability, echeloning, provision of spare parts and the need to put into operation an effective information system that provides an up-to-date overview of stocks in real time and place.

Question 2 for enlisted/ civilian maintenance personnel and NCOs, and question No3 for officers: "To what extent do you think that depots in military units store enough parts for all weapons systems and types of equipment in order to perform the necessary maintenance and repairs?"

Question 3 for enlisted personnel and NCOs and Question 4 for officers: "To what extent do you think there is a clear echeloning of spare parts for carrying out repairs depending on the rights and competencies of the same by technical personnel at different levels?"

Question 4 for enlisted/civilian maintenance personnel: „To what extent do you think you have been supplied on time with spare parts and exploitation materials for the maintenance and repair activities you carry out?“

Question 4 for NCOs and Question 5 for officers: “To what extent do you think that the requests made by you for the allocation of spare parts and operational materials are provided (on time and in the required volume and quality)?”.

Question No. 5 for enlisted personnel and NCOs and question No. 6 for officers: "To what extent do you think it is absolutely imperative that an information system is installed in the units at all levels to provide up-to-date information on stock availability of spare parts, nodes and units and a tracking technical system for W&E throughout the whole life cycle?"

The results for the questions in Fig. 3.1., Fig. 3.2. and Fig. 3.3., indicate that the majority of the respondents (over 72% of the officers, 54% of the NCOs and 52% of the enlisted/civilian personnel) believe that they have not been provided the necessary spare parts to ensure the repairs. This slows down the repair process a lot and in many cases the equipment cannot be used for a long period of time and awaits public tender procedures or the delivery of a part.

In a similar way, but less categorically, 35% of the NCOs, 34% of the enlisted/civilian personnel, but categorically more than 51% of the officers, state that there is no clear allocation of the parts for the repairs in the units depending on their abilities to perform the types of repairs. This leads to the lack of certain parts in the units performing certain repairs and the availability of such parts for repairs in units that cannot perform those repairs and vice versa. In addition, it is unequivocally stated by almost all surveyed categories that the spare parts request forms are not provided within the specified period and volume. Over 55% of non-commissioned officers and enlisted/civilian personnel and over 63% of officers say it is imperative to integrate a functioning information system within the repair production process that provides real-time information about the availability of resources.

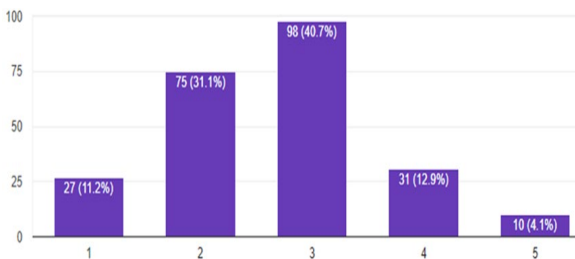


Fig. 3.1. Responses to Question 4 for enlisted/civilian maintenance personnel.

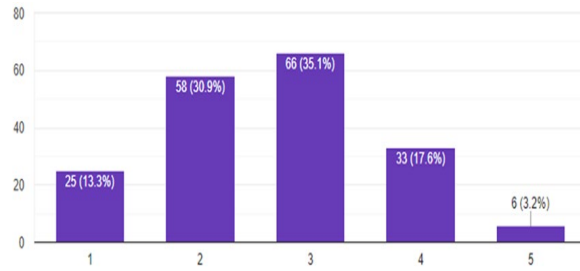


Fig. 3.2. Responses to Question 4 for NCOs.

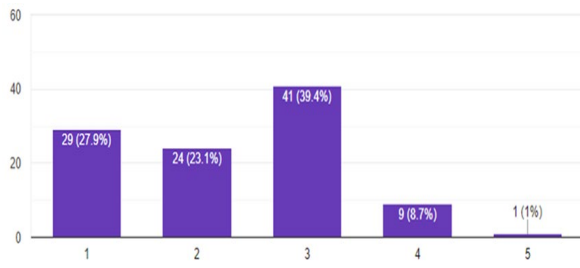


Fig. 3.3. Responses to Question 5 for officers..

Question 6 for enlisted/civilian personnel and NCOs and Question 7 of the commissioned officers survey reads as follows: “To what extent do you believe that logistics supply through contracts has a direct impact on the quality and timely maintenance and repair of W &E?”

The analysis of the responses this question shows that more than 50% of the enlisted personnel, 40% of the NCOs and 60% of the officers state that the relationship between the contracts for logistics supply of resources and services and the performance of quality and timely maintenance and repair is extremely important. Without the provision of a constant flow of spare parts provided by the contracts, it is not possible to carry out timely repair activities. A significant number of the public procurement tender procedures without direct negotiation takes an extremely long time, and in some cases the requested spare parts are simply not supplied by the contractor because the price initially provided is unrealistically low in order to win the contract. These parts are not supplied and a minimal penalty is paid for doing so. In other cases, public tenders fail due to a lack of candidates, or after being won, those who failed the procedure appeal and thus stop its implementation for a long time. An appropriate solution to these problems is to provide the unit commanders with more legal opportunities for direct negotiation, and not only legal entities of budgetary support, but also the low tactical levels. This would give greater freedom to make decisions that are critical to maintaining military capabilities.

Questions 7, 8, and 9 of the enlisted/civilian personnel and NCO surveys are identical to Questions 8, 9, and 10 for officers referring to the provision, condition, and modernization of the facilities, depots and technological equipment with the performance of quality and timely maintenance and repair and read as follows:

Question 7 for enlisted personnel and NCOs and Question 8 for officers: "To what extent do you think that the provision of adequate infrastructure and appropriate technological equipment has a direct impact on the quality and timely maintenance and repair of W&E?"

Question 8 for enlisted personnel and NCOs and Question 9 for officers: "To what extent do you think modernization of the facilities/depots and technological equipment is needed?"

Question 9 for enlisted personnel and NCOs and Question 10 for officers: "To what extent do you think that the warehouses for storing armoured vehicles and artillery armament meet the storage requirements for new W and E?"

Question 10 for enlisted/civilian maintenance personnel is specific to the respondent category: "To what extent do you feel that you are provided with the equipment (in the appropriate operation condition and sufficient quantities) necessary for your maintenance and repair activities?"

The analysis of the responses to the above questions shows that more than 57% of the enlisted/civilian personnel, 63% of the NCOs and 77% of the officers share the opinion that the infrastructure development and the provision of the appropriate technological equipment are of key importance for carrying out quality maintenance and repair. The enlisted/civilian personnel who answered Question 10 believe that they do not have enough operational equipment to be able to fully perform the activities required for performing quality maintenance and repair. The experience of the leading armies in the Alliance shows that quality maintenance and repair go hand in hand with the development of the infrastructure and the provision of adequate equipment. This means that swift action is to be taken so that the infrastructure and supplies necessary for carrying out maintenance and repair of the equipment and armament in the Bulgarian Armed Forces are provided.

The respondents unanimously agree about the need for modernization of the facilities and equipment. The results of the questions are shown in Fig. 4.1., Fig. 4.2. and Fig. 4.3. Over 79% of enlisted/civilian personnel, 86% of NCOs, and 92% of officers believe that the modernization, which has been long overdue, is imperative. The modern realities dictated by changes in the security environment show the need to acquire new capabilities not only in terms of equipment and weapons, but also in terms of facilities and technological equipment where maintenance and repairs are carried out. Another important aspect is the development of mobile technical support modules equipped with the appropriate apparatus for on-site diagnostics and repair.

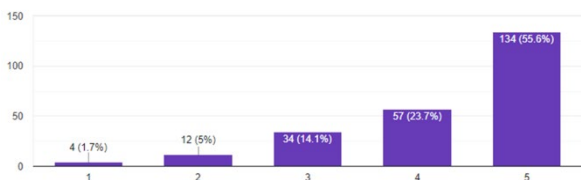


Fig. 4.1. Responses to Question 8 for enlisted/civilian maintenance personnel.

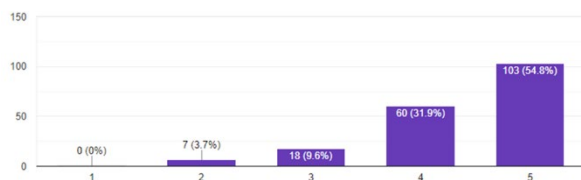


Fig. 4.2. Responses to Question 8 for NCOs

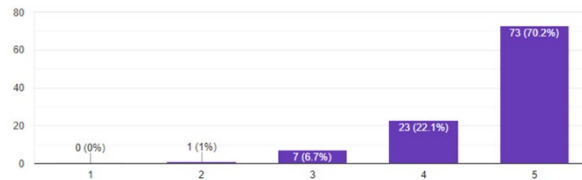


Fig. 4.3. Responses to Question 9 for officers

An important aspect of the maintenance and repair system is the stock availability of spare parts, nodes, units, and operating materials needed for maintenance and repair. The answers of the respondents regarding the condition of the storage facilities for armored vehicles and artillery armament indicate that in reality these facilities do not fully comply with the requirements for the newer models of W and E.

Questions 11 to 16 of the enlisted/civilian personnel survey, Questions 10 to 14 of the NCOs survey, and Questions 11 to 15 of the commissioned officers survey focus on the organization of the technological process of maintenance, the correspondence between the repairs and the hierarchical level of the repair structure, as well as the provision of the necessary technical documentation. Part of the answers to these questions are shown in Fig. 5.1., 5.2., and 5.3.

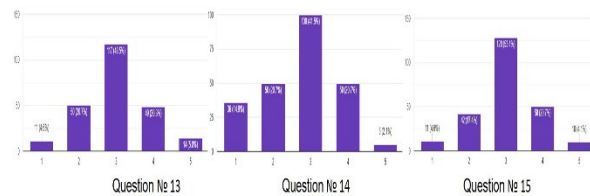


Fig. 5.1. Responses to Questions 13, 14, and 15 for enlisted/civilian maintenance personnel

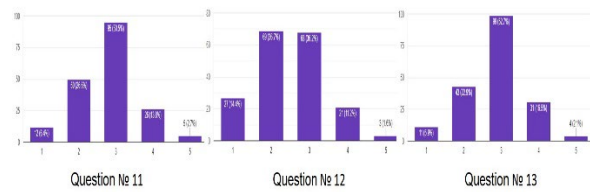


Fig. 5.2. Responses to Questions 11, 12, and 13 for NCOs

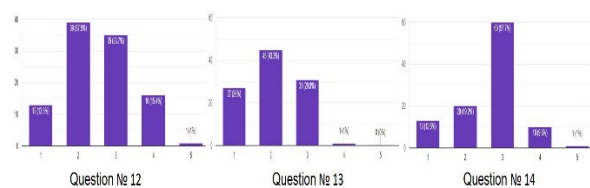


Fig. 5.3. Responses to Questions 12, 13, and 14 for officers.

‘Question 11 of the enlisted/civilian personnel and officers surveys and Question 10 of the NCOs survey are identical and read as follows:

"To what extent do you think the technological process of the repairs is properly organized in terms of type and complexity?"

The analysis of the answers to the question shows a hesitation in all the surveyed categories, who cannot clearly express an opinion on the matter.

Question 12 of the enlisted/civilian personnel survey is specific to the category and reads as follows:

"To what extent do you feel you are familiar with the overall process of acceptance, repair and delivery of W&E?"

A review of the responses to this question indicates that most enlisted/civilian personnel surveyed are familiar with the W&E delivery and repair process. However, about 15% state that they have little knowledge of the entire recovery process, which necessitates the appropriate training and courses in order for such omissions to be eliminated.

Question 13 of the enlisted/civilian maintenance personnel survey, Question 11 of the NCO survey, and Question 12 of the commissioned officers survey are identical and read as follows:

"To what extent do you think the level of production equipment matches the level of the repair structure (platoon, company, battalion, regiment/base)?"

The answers to the questions show that the enlisted/civilian maintenance personnel cannot express a clear opinion about the conformity of the technological equipment with the level of the repair structure. However, the higher we rise in the hierarchy of the military profession, the more clearly the respondents tend to express their opinion about this discrepancy. Thus, we arrive at the opinion of the officers, of which more than 50% strongly believe that the production equipment does not correspond to the level of the specific repair structure and that it is imperative for it to be reviewed and minimized in order to clearly define the repair activities at the relevant levels in accordance with the available equipment and repair parts.

Question 14 of the enlisted/civilian repair personnel survey, Question 12 of the NCO survey, and Question 13 of the commissioned officers survey are identical and read as follows:

"To what extent do you think that there is sufficient technical documentation, calibers and spare parts for the maintenance and repair of the new W & E models commissioned in recent years?"

Question 15 of the enlisted/civilian repair personnel survey, Question 13 of the NCO survey, and Question 14 of the commissioned officers survey are identical and read as follows:

"To what extent do you think that the regulatory documents and procedures for maintenance and repair are properly echeloned at the different levels (appropriate design of the technological process and equipment depending on the repairs being carried out)?"

The analyzed responses to this question show a similar linear correlation between the forthrightness of the negative opinion of the respondents and the climbing up the pyramid of military hierarchy. Thus, if the percentage of enlisted/civilian maintenance personnel who expressed their opinion that there is a shortage of documentation and spare parts is 35, then for NCOs this percentage increases to 50, and for officers it soars to 75. This trend clearly shows that the higher up the ladder of the military maintenance and repair hierarchy a person stands, the

more clearly they see the overall picture the general trends in the development of the maintenance and repair system in the armed forces.

Analogous, but not so clearly expressed, are the answers given to the question related to the appropriate design of the technological process and equipment depending on the repairs being carried out. The respondents indicate, although not so categorically, the inconsistency in the structuring of the technological process depending on the performed repair activities.

Question 16 of the enlisted/civilian repair personnel survey, Question 14 of the NCO survey, and Question 15 of the commissioned officers survey are identical and read as follows:

"To what extent do you think that you have been provided with the necessary technical documentation for the activities you perform/ that you have been provided with the necessary documentation supporting maintenance and repair (e.g. technology maps)?"

A careful examination of the responses to the question under consideration shows that while the enlisted/civilian repair personnel think that they have the necessary documentation for the repair work they carry out, the NCOs and officers believe the opposite, expressing the opinion that there is a significant lack of such documentation. Their disagreement is probably due to the fact that they are the ones who seek out and provide the necessary technical documentation for the enlisted/civilians to carry out the repair activities. The process of modernization of our armed forces should also include the acquisition of maintenance and repair capabilities of the newly commissioned W & E models, while at the same time acquiring the necessary technical documentation related to them.

The next group of questions by categories of technical specialists examines the state of their training and its impact on the performance of quality maintenance and repair.

Question 17 of the enlisted/civilian repair personnel survey, Question 15 of the NCO survey, and Question 16 of the commissioned officers survey are identical and concern the level of training of technical personnel (Fig. 6), reading as follows:

"To what extent do you think that the training of technical specialists affects the quality of the maintenance and repair of W & E?"

The responses to the question show an absolute consolidation between the different categories of respondents around the opinion that the quality of the performed maintenance and repair activities are directly proportional to the training of the personnel who perform them. Preparation is the cornerstone of any endeavor, especially when it comes to handling and maintenance of B&T.

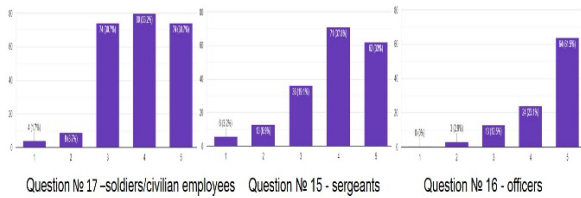


Fig. 6.. Responses to Question 17 of the enlisted/civilian repair personnel survey, Question 15 of the NCO survey, and Question 16 of the commissioned officers survey

Question 18 of the enlisted/civilian repair personnel survey, Question 16 of the NCO survey, and Question 17 of the commissioned officers survey (Fig. 7) are identical and refer to the respondents' opinion regarding the standardization of training of technical personnel, reading as follows:

"To what extent do you think the training of technicians should be standardized since it affects the quality of W & E maintenance and repair?"

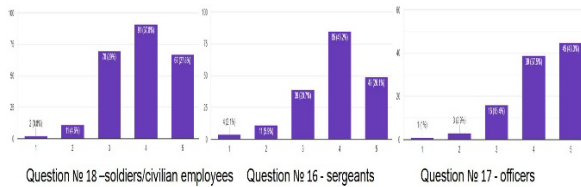


Fig. 7.. Responses to Question 18 of the enlisted/civilian repair personnel survey, Question 16 of the NCO survey, and Question 17 of the commissioned officers survey.

The analysis of the results on the examined issue clearly shows again the unanimous opinion of the respondents. Over 65% of enlisted/civilian personnel surveyed, 71% of NCOs and 80% of officers believe that it is imperative to standardize the training of technicians in order to standardize the level knowledge and skills they acquire for the operation, maintenance and repair of W & E in accordance with the current educational requirements and the requirements of stakeholders. In the years of reforms in the armed forces, the military education system was inevitably affected, which led to a difference in the level of training of the various categories of technical specialists, especially enlisted personnel and NCOs. The differences in the training requirements for technical specialists in the individual units led to significant challenges when implementing uniform educational standards and difficulties in carrying out maintenance and repair, especially of the new W & E models. This necessitates the standardization of the training of the individual categories of technical specialists which is to be achieved by conducting it in one location, by applying the same criteria and by ensuring of acquired knowledge and skills are on the same level.

Question 19 of the enlisted/civilian repair personnel survey, Question 17 of the NCO survey, and Question 18 of the commissioned officers survey identically refer to the training of depot personnel and read as follows:

"To what extent do you think that the depot personnel/depot managers have sufficient technical training?"

The analysis of the responses to this question indicates that more than half of all categories surveyed (51% of enlisted/civilian maintenance personnel, 69% of NCOs

and 50% of officers) believe that depot personnel possess the necessary technical qualifications to perform their official duties.

Question 20 of the enlisted/civilian repair personnel survey, Question 18 of the NCOs survey, and Question 19 of the commissioned officers survey refer to the specific competences of the maintenance and repair specialists read as follows:

Question 20 of the enlisted/civilian maintenance personnel: "To what extent do you think you have the necessary special training for the activities you perform as technical specialist for the repair/maintenance of...?"

Question 18 of the NCOs survey and Question 19 of the commissioned officers survey: "To what extent do you think that operating, maintenance and repair personnel have undergone the necessary specialized training?"

The responses to those questions make it clear that more than 53% of the operating and maintenance staff are of the opinion that they have obtained the necessary knowledge and skills for the activities they perform. The same opinion is supported by their commanders and superiors - more than 53% of the NCOs and 58% of the officers believe that their subordinates possess the necessary specialized competencies.

The following Question 21 of the enlisted/civilian maintenance personnel survey, Question 17 of the NCOs survey, and Question 18 of the commissioned officers survey are identical for all categories and read as follows:

"To what extent do you think that the damage to the weaponry and equipment is the result of the incorrect operation and incomplete maintenance?"

In the answers to this question, the enlisted/civilian maintenance personnel could not express a clear opinion, while the NCOs (more than 34%) and officers (more than 55%) have arrived at the conclusion that the damage to W & E is a consequence of the deficiencies in its maintenance.

Question 22 of the enlisted/civilian maintenance personnel survey, Question 20 of the NCOs survey, and Question 21 of the commissioned officers survey are identical for all surveyed categories and reflect the opinion of the respondents regarding the availability of courses for technical specialists and read as follows:

"To what extent do you think there are sufficient qualification courses for technical specialists?"

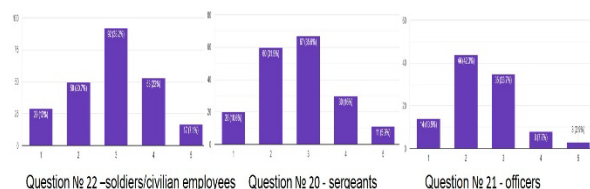


Fig. 8.. Responses to Question 22 of the enlisted/civilian maintenance personnel survey, Question 20 of the NCOs survey, and Question 21 of the commissioned officers survey.

In their responses to this question, the interviewed categories share the opinion that the courses for technical specialists are not enough and it is necessary to provide more opportunities for increasing the qualification, not only for the maintenance and repair of the old W & E, but

also for what to be commissioned in the Bulgarian Armed Forces in the future. When preparing the plans for the modernization of the armed forces, it is necessary to take into account not only the one-time act of acquiring W & E, but the entire life cycle of their use, including the training of maintenance and repair technical specialists and operating personnel, as well as the construction of infrastructure and technological equipment for maintenance and repair activities. In addition, it is necessary that these plans provide for samples of the newly acquired equipment, training labs, simulators and documentation to be mandatorily provided for the military educational institutions so that the future officers and NCOs have the opportunity to acquire the necessary knowledge and skills for the operation, maintenance and repair of new the samples. Thus, they will be able get to know it and handle it skillfully, as well as manage the overall processes of conducting all relevant activities. The experience of concluding similar contracts, such as the acquisition of transport equipment from the Mercedes brand, can serv as a lesson learned on how such contracts should not be concluded as far as maintenance and repair are concerned. This shows the need for taking the necessary measures to minimize such errors and for paying particular attention to the training of technical specialists through a sufficient number and variety of courses that cover the entire spectrum of W & E in exploitation by the BAF.

Question 21 of the NCOs survey is identical to Question 22 of the commissioned officers survey and reads as follows:

"To what extent do you think your subordinates have the necessary competencies for the maintenance and repair activities they perform?"

The analysis of the answers to the above question shows that over 44% of the NCOs and 56% of the officers express to a relatively high and very high degree the opinion that the personnel at their disposal has the necessary knowledge and skills to perform their official duties.

Question 23 of the enlisted/civilian maintenance personnel survey is identical to Question 22 of the NCOs survey and Question 23 of the commissioned officers survey and reads as follows:

"To what extent do you think there is a clear distribution of activities for the types of W & E repairs at the different hierarchical levels?"

Almost half of all respondents cannot formulate a clear opinion on this question. However, 34% of enlisted/civilian maintenance personnel claim that they believe that the distribution of maintenance activities across hierarchical levels is clearly structured, compared to 26% of noncommissioned officers and only 21% of officers. This raises the issue of revising and clearly differentiating the activities pertaining to the several types of military repairs at the different hierarchical levels together with the technological equipment and spare parts for their performance. This will allow for reducing not only the number of uncharacteristic activities when carrying out simple repairs at the upper levels or complex

ones at the lower levels, but also the use of spare parts stored in the warehouses of the repair structures that are not capable or required to carry out repairs using them.

The following question is the same for all categories surveyed (Question 24 for the enlisted/civilian maintenance personnel, Question 23 for NCOs, and Question 24 for officers) and is related to the previous question, reading as follows:

"To what extent do you think the repair needs correspond to the level of the repair structure (platoon, company, battalion, regiment/base)?"

The results of the answers to this question are similar to the previous one. The percentage of undecidedness in the opinion of the interviewees is high; however, while among the enlisted/civilian maintenance personnel the prevailing opinion is that the repair needs correspond to the level of the structure, the opinion of the officers is the polar opposite. Officers have a view of the overall repair process while enlisted personnel do not have this perspective, which is why it is necessary to reassess the need for repair in line with the structure level.

The final Question 25 is specific only for enlisted/civilian maintenance personnel, as it concerns the equitable division of labor:

"To what extent do you think that the maintenance and repair tasks performed are properly/evenly distributed among the technicians?"

More than 40% of the respondents to this question are of the prevailing opinion that the distribution of activities between technical specialists is fair. This issue is important because if this rule is not followed according to Adams' theory of justice [1], negative injustice will occur, which will lead to tension and even anger in the team performing the repair activities. This, in turn, can lead to a decrease of performance efficiency when carrying out their duties. For this reason, immediate superiors need to strive for an even distribution of maintenance and repair activities among technicians.

#### IV. CONCLUSIONS

The following conclusions can be drawn from the study of the operation, maintenance and repair system in the Armed Forces of the Republic of Bulgaria, the analysis of the results obtained during its carrying out, as well as the results from previous research:

**The first conclusion** is that all surveyed categories unanimously indicate the supply of material resources as a factor of key importance in performing quality and timely maintenance and repair of W & E. In addition, this functional area of logistics together with Movement and Transportation, Management of Logistics Information and Military Infrastructure Provision are the cornerstones of W & E maintenance. The spare parts and operational materials are of particular importance for timely maintenance and repair. However, these are often unavailable or not delivered on time due to problems arising during the public procurement procedures or the conclusion and execution of contracts. The analyzed results of the study indicate that it is the supply of material



resources, as an element of the studied operation, maintenance and repair system, that plays a primary role on the overall condition of this system, which requires improvement of supply procedures and optimization of the connections between the two functional areas - supply and repair.

**The second conclusion** is related to the training of the technical personnel.

The analysis of the results on the relevant issues shows a thesis presented in previous studies [4] that standardization is a key factor for improving the training of technical specialists. All categories of respondents share the opinion that the quality of maintenance and repair activities is inextricably linked to the training of the personnel who perform them. The differences in the level of training carried out in the individual units lead to significant difficulties in meeting uniform educational criteria and this is the rationale behind the need for standardization. This standardization is to be achieved by centralizing and conducting training in the military education institutions as well as by subjecting the trainees to the same training criteria in order for them to acquire knowledge and skills that are on the same level. All the interviewed categories unanimously uphold that personnel should be provided with more opportunities to increase their qualification through attending various courses. The scope of those courses should include not only the maintenance and repair of the old W & E, but also W & E that is to be acquired and implemented by the Bulgarian Armed Forces in the future. Samples of the new equipment should be provided complete with the necessary technical documentation and training labs to the military educational institutions, which provide the fundamentals of training in the armed forces.

**The third conclusion** of the conducted research shows an unclear echeloning of the production equipment, as well as of the spare parts for carrying out the repair activities in the units of the individual levels in accordance with their capabilities to carry out the various types of repairs. Ensuring the appropriate design of the overall technological process in accordance with the level of the repair structure and the duties relating to the specific type of repairs, together with the necessary spare parts, will lead to an increase in the effectiveness and efficiency of the maintenance and repair system by avoiding duplication of efforts and reducing unnecessary stock surplus.

The issues related to the maintenance and repair of weaponry and equipment are reflected annually in the reports on the state of defence, [5], [6], [7], [8] and in the scientific works of various researchers. However, there is still no correct formula for resolving these issues, and their solutions continue to be deferred. It is necessary to apply a unified radical approach to all elements of the entire logistics system while taking into account all the interdependencies and correlations between them as listed in the above conclusions.

The operation, maintenance and repair system is a subsystem of the overall logistics system, and not merely a functional area within it. If the overall system for logistics support, built up from its elements that perform the various logistics functions (the functional areas of logistics), is viewed through the prism of the system approach, then the change in the state of each element of the system would lead to a change in the state of the entire system.

The research conducted examined the influence of the remaining logistics functions on operation, maintenance and repair as elements of one system. The analysis of the results of the conducted research led to the above-mentioned main conclusions, on the basis of which it can be said that maintenance and repair are clearly dependent on the supply function, on the training of technical specialists and on the structure of the technological process of maintenance and repair, as well as on the structure and responsibilities of the technical staff of the various hierarchical levels. What stands out prominently is the need to improve the current system for the maintenance and repair of W & E by taking urgent measures to eliminate the identified problems in order to optimize the overall system for logistics provision.

#### ACKNOWLEDGMENTS

The publication of the article was financed with funds provided by the National Security and Defence Science Program.

#### REFERENCES

- [1] J. Adams, Toward an Understanding of inequity, *Journal of Abnormal and Social Psychology*, 1963, pp. 422-436
- [2] *Doctrine for Logistics (NP-04)*, edition (A), MoD, Sofia, 2019, p. 13
- [3] I. Malamov, G. Grigorov, The State of the System for Operation, Maintenance and Repair in the Armed Forces of the Republic of Bulgaria, Scientific conference "Logistics and Public Systems", February 25-27, 2021, Veliko Tamovo, Vasil Levski NMU Publishing, ISSN 2738-804, Pages 14
- [4] I. Malamov, Influence of the Technical Specialists' Training on the System for Maintenance and Repair of Weaponry and Equipment of the Armed Forces of the Republic of Bulgaria. Collection of papers from the university scientific conference, "Logistics and Public Systems", 16-17. March 2023, Vol. 1, ISSN:2739-8034, Vasil Levski NMU Publishing, Veliko Tamovo, 2023
- [5] Report on the State of Defence and the Armed Forces of the Republic of Bulgaria 2018, adopted by the Council of Ministers with Decision No 232 from 25 April 2019, MoD, Sofia, 2019, p. 29
- [6] Report on the State of Defence and the Armed Forces of the Republic of Bulgaria 2019, promulgated in State Gazette, issue 50 from 2 June 2020, MoD, Sofia, 2020, p. 49
- [7] Report on the State of Defence and the Armed Forces of the Republic of Bulgaria 2021, adopted by the Council of Ministers with Decision 295 from 02 April 2023, p. 47
- [8] Report on the State of Defence and the Armed Forces of the Republic of Bulgaria 2022, adopted by the Council of Ministers with Decision 253 from 03 April 2023, MoD, Sofia, 2022, p. 39



*Professor, leading researcher Dr.habil.geol. Gotfrīds Noviks*  
(15/09/1935 – 07/03/2024)

Professor Gotfrīds Noviks worked at Rezekne Academy of Technologies (RTA) since the establishment of the education institution. A lot of work was devoted to further development of the Academy. Professor Noviks was the scientist: habilitated doctor of geology, vice-rector of the Science and Studies Department, head of the Department of Natural and Engineering Sciences, creator of environmental engineering study programs and program director at the bachelor's, master's and doctoral levels. He prepared more than 320 scientific publications, obtained 25 authorship certificates, participated in more than 100 scientific conferences, led scientific projects and research groups. Professor was the initiator of the scientific conference "Environment. Technology. Resources" where the scientists and researchers from foreign countries and Latvia have been participating for many years. Professor's pedagogical experience lasted for almost 60 years. He was also the author of many textbooks which are still used in many countries of the world. Professor Noviks was the founder of rock physics, the author of the first textbook "Fundamentals of Rock Physics" which was the first one in this field in the former Soviet Union. He was the member of the International Water Federation (WEF) from 1995, the member of the ecological committee and ecological education committee from 1996, the member of the New York Academy of Sciences.

Gotfrīds Noviks was born in Ludza, graduated from Viļani Secondary School, later from Leningrad Institute of Mining, where he studied geology. In the scientific field, he worked at the Moscow Mining Institute in Russia, then at the Kabul Polytechnic Institute in Afghanistan for a short period. Afterwards he decided to return to Latvia, responding to an invitation to work in Rezekne. In 1994, Professor Noviks started to work at Rezekne Higher Education Institute (now Rezekne Academy of Technologies).

He worked at the Rezekne Academy of Technologies, led the scientific work, as well as enjoyed the hobbies that brought a lot of joy and inspiration for him. Gotfrīds Noviks once admitted that his hobby was kayak trips on rivers. His idea of ecological expeditions for 1st-year students of the environmental engineering still lives on. The first expedition was organized in 1997. Professor told that he liked reading books, cooking; he was interested in photography, enjoyed the nature with forests, rivers, and mountains as well.