



International forum
**SAFETY FOR
THE FUTURE**

SoCMan
SECURITY AND CRISIS MANAGEMENT - THEORY AND PRACTICE

IX INTERNATIONAL FORUM „SAFETY FOR THE FUTURE 2023“

IX INTERNATIONAL SCIENTIFIC - PROFESSIONAL CONFERENCE

SECURITY AND CRISIS MANAGEMENT - THEORY AND PRACTICE

PROCEEDINGS



IX INTERNATIONAL FORUM „SAFETY FOR THE FUTURE 2023”

IX Scientific-professional conference
SECURITY AND CRISIS MANAGEMENT -THEORY AND PRACTICE
(SeCMan)

September 29th and 30th, 2023 Belgrade, Republic of Serbia

FOREWORD

*The international forum **Safety for the Future** arose from the idea and the need to see security problems, and yet separately, through a prism of scientists and experts to bring science, company practice and economy together. The forum contains several important events: the International Scientific Conference "Security and Crisis Management-Theory and Practice", various lectures and workshops, an exhibition of tools and equipment, demonstration exercises on the usage of different assets and equipment in various security activities and numerous debates and discussions with a variety of topics.*

This year, for the ninth time, we are holding the conference "Security and Crisis Management-Theory and Practice", with new elements of researching security phenomena in the field of crisis management, but also including all related areas. The fact is that the environment in which individuals and legal entities exist is increasingly complex, and the range of phenomena that affect the security of an entity is becoming wider. It consists of familiar and unfamiliar circumstances. Managing those circumstances is possible to a certain extent if there is an optimal and necessary quantum of knowledge. Hence, knowledge is the foundation on which is necessary to build the capabilities of individuals and legal entities to be able to recognize, prevent and react to threats.

Crisis management has become an everyday need, essential for the survival of individuals, companies, or society. It is more and more difficult to assess the risk of events with negative effects at the very beginning of their occurrence, and coping with negative consequences leaves harder effects on society. Scientific research of security phenomena has become the priority of society's sustainable development. Scientific knowledge is necessary for systematic knowledge of phenomena in the environment and practice for checking their usability.

Scientific findings do not always come to those who perform security tasks, such as individuals or legal entities. Therefore, there is a need for scientists and experts to meet and exchange ideas, opinions, and knowledge. Materialization of knowledge is carried out daily in the process of modern business and management. Exposed to the impacts of a turbulent environment and focused on sustainability, modern business and management require permanent monitoring of changes and adaptation to these changes.

Comprehension of the environment in which modern society exists is possible if there is the necessary knowledge of the phenomena that characterize it. That knowledge provides an opportunity for preventive action through an efficient risk assessment system. Only knowledge, formed as a symbiosis of science and profession, has quality and strength, which guarantees the possibility of preventive action and an optimal level of readiness to react to negative events. The resistance of contemporary society to negative events depends on the degree of knowledge development.

*This year's conference is organized in specific conditions, due to increased danger of a world nuclear conflict. Namely, the world is still facing a serious risk of an outbreak of armed conflict on a global scale. Not analyzing the necessity of solving international disputes through war, it is the fact that in the year 2023 we are standing on the edge of possible war between the Russian Federation and NATO. That automatically implies conflict on a global level. The special military operation, conducted by the Russian Federation on the Ukrainian territory (which lasts more than 500 days), has even strongly triggered a sequence of events which affect the security of the whole world (economy, demography, energy, finances, etc.). This crisis is just another proof that forum **Safety for the Future** properly observes the complexity of the security environment and steers it towards crisis management. Bearing in mind that it is not possible to put all the problems in one Proceedings or to answer all the questions, the*

forum will continue to deal with the contemporary security challenges, risks, and threats in the future, as well.

Proceedings from the IX International Conference — Security and Crisis Management — Theory and Practice, present a new value in the observation of a portfolio of security phenomena at the strategic, company, and individual levels. The papers published in the proceedings are new findings and views of the authors. A wide range of issues confirms the assumption of the necessity of such a conference. The papers presented at the last eight conferences have unambiguously demonstrated the need for regional cooperation and the harmonization of joint capacities. And spreading knowledge becomes a priority in the development of a security culture.

The forum represents a review of existing knowledge, a source of new knowledge, assistance to researchers and practitioners in solving security problems, support for those who practically deal with security and a source of an initiative to improve existing knowledge in the field of security, management, and engineering.

Besides the conference, throughout the other events and by analyzing different occurrences, the forum contributes further spreading of security culture and merging of theory and practice.

We hereby invite all interested scientists and professionals to improve the quality of future publications with their papers.

Program Committee

PROGRAM COMMITTEE

- Branko Babic PhD, *Higher Technical School of Professional Studies, Novi Sad - Chairman*
- Aleksandar Andrejevic PhD, *EDUCONS University, Sremska Kamenica, Serbia*
- Andrea Andrejevic Panic PhD, *EDUCONS University, Sremska Kamenica, Serbia*
- Goran Andjelic PhD, *EDUKONS University, Faculty of Security Studies, Sremska Kamenica, Serbia*
- Darko Bozanic PhD, *University of Defense, Military Academy, Belgrade, Serbia*
- Marijan Brozovic PhD, *Polytechnic of Karlovac, Croatia*
- Ruggiero Cafari Panico PhD, *Full Professor of European Union Law, University of Milan, Italy*
- Gian Luigi Cecchini PhD, *Full Professor of European Union Law, University of Trieste, Italy*
- Sinisa Domazet PhD, *EDUCONS University, Faculty of Security Studies, Sremska Kamenica, Serbia*
- Drazan Erkcic PhD, *The Republic of Srpska Ministry of the Interior - Police Administration Zvornik, Bosnia and Herzegovina*
- Tatjana Gerginova PhD, *University of St. Kliment Ohridski, Faculty of Security Skopje, Northern Macedonia*
- Ljubomir Gigovic PhD, *University of Defense, Military Academy, Belgrade, Serbia*
- Ladin Gostimirovic PhD, *College of Business and Technical Education, Doboj, Bosnia and Herzegovina*
- Emina Hadzic Dreznjak PhD, *University of Sarajevo, Faculty of Civil Engineering, Bosnia and Herzegovina*
- Predrag Ilic PhD, *Institute for Protection, Ecology and Informatics, Banja Luka, Republika Srpska, Bosnia and Herzegovina*
- Zeljko Ilic PhD, *Republic Administration CZ, Republika Srpska, Bosnia and Herzegovina*
- Vladimir Jakovljevic PhD, *University of Belgrade, Faculty of Security, Belgrade, Serbia*
- Jelena Jesic PhD, *EDUCONS University, Sremska Kamenica, Serbia*
- Radislav Jovicic PhD, *Business and Technical College, Doboj, Bosnia and Herzegovina*
- Dragisa Jurisic PhD, *Security Research Center, Banja Luka, Republika Srpska, Bosnia and Herzegovina*
- Samed Karovic PhD, *EDUCONS University, Faculty of Security Studies, Sremska Kamenica, Serbia*
- Milica Mladenovic PhD, *S4 Glosec Global Security, Belgrade, Serbia*
- Savo Kentera PhD, *Atlantic Alliance of Montenegro, Podgorica, Montenegro*
- Nenad Komazec PhD, *University of Defense, Military Academy, Belgrade, Serbia*
- Tomaz Kramberger PhD, *University of Maribor, Faculty of Logistics Celje, Slovenia*
- Mirjana Laban PhD, *University of Novi Sad, Faculty of Technical Sciences, Novi Sad, Serbia*
- Ivona Shushak Lozanovska PhD, *Faculty of Law, St. Kliment Ohridski University Bitola, Northern Macedonia*

Goran Maksimovic PhD, *Security Research Center Banja Luka, Republika Srpska, Bosnia and Herzegovina*

Nada Marstijepovic PhD, *Faculty of Maritime Studies, Kotor, Montenegro*

Marina Mihajlovic PhD, *University of Belgrade, Faculty of Technology and Metallurgy, Innovation Center, Belgrade, Serbia*

Aleksandar Milic PhD, *University of Defense, Military Academy, Belgrade, Serbia*

Branislav Milosavljevic PhD, *University of UNION Nikola Tesla, Faculty of Business Studies and Law, Belgrade, Serbia*

Dragan Mladjan PhD, *Criminal Police University, Belgrade, Serbia*

Nenad Mustapic PhD, *Polytechnic of Karlovac, Croatia*

Vesna Nikolic PhD, *University of Nis, Faculty of Occupational Safety Nis, Serbia*

Dragan Pamucar PhD, *University of Belgrade, Faculty of Organizational Sciences, Belgrade, Serbia*

Ruggiero Cafari Panico PhD, *Full Professor of European Union Law, University of Milan, Italy*

Aca Randjelovic PhD, *University of UNION Nikola Tesla, Faculty of Business Studies and Law, Belgrade, Serbia*

Tomislav Radovic PhD, *Faculty of Management Zajecar, Megatrend University, Belgrade, Serbia*

Momcilo Sakan PhD, *Independent University of Banja Luka, Bosnia and Herzegovina*

Slobodan Simic PhD, *Security Research Center Banja Luka, Republika Srpska, Bosnia and Herzegovina*

Augusto Sinagra PhD, *European Union Law, University of Rome "La Sapienza"*

Miomir Stankovic PhD, *University of Nis, Faculty of Occupational Safety Nis, Serbia*

Katarina Strbac PhD, *Faculty of Engineering Management, Belgrade, Serbia*

Jovan Vucinic PhD, *Polytechnic of Karlovac, Croatia*

Nahla Yassine-Hamdan PhD, *American University in the Emirates, College for security and global studies, Dubai, United Arab Emirates*

Dusko Tomic PhD, *American University in the Emirates, College for security and global studies, Dubai, United Arab Emirates*

Eldar Saljic PhD, *American University in the Emirates, College for security and global studies, Dubai, United Arab Emirates*

Dr.h.c.. mult. Mgr. JUDr. Jozef Zařko, PhD., MBA, LL.M, Honor. Prof. mult., *Európsky inštitút d'alsieho vzdelávania, Podhájska, Slovensko*

Peter Plavcan PhD, *Danubius University, Sládkovicovo, Slovak Republic*

Marija Vukic PhD, *IRC Alfatec, Nis, Serbia*

Zeljko Zoric PhD, *Sector Security Company, Banja Luka, Republika Srpska, Bosnia and Herzegovina*

Dragana Kosic Msc, *Sector Security Company, Banja Luka, Republic of Srpska, Bosnia and Herzegovina*

Tatjana Bojanic, *Institute for Standardization of Serbia, Belgrade, Serbia*

ORGANIZING COMMITTEE

Milica Mladenovic, PhD, *S4 GLOSEC Global Security, Belgrade, Serbia, Chairman*

Slavica Dabizljevic, PhD candidate, *RASEC, Belgrade, Serbia*

Maja Mijatovic, MSc, *S4 GLOSEC Global Security, Belgrade, Serbia*

IMPRESSUM

Editorial

Komazec Nenad, PhD, Belgrade, Serbia
Babic Branko, PhD, Novi Sad, Serbia
Dragan Mladjan, PhD, Belgrade, Serbia

Publisher

Regional Association for Security and Crisis Management-RASEC
S4 GLOSEC Global Security

Reviewers

Kramberger Tomaz, PhD – Slovenia
Karovic Samed, PhD – Serbia
Strbac Katarina, PhD – Serbia
Pamucar Dragan, PhD – Serbia
Babic Branko, PhD – Serbia
Jurisic Dragisa, PhD – Bosnia and Herzegovina
Bozanic Darko, PhD – Serbia
Komazec Nenad, PhD – Serbia
Maksimovic Goran, PhD – Bosnia and Herzegovina
Tatjana Gerginova, PhD – North Macedonia
Milic Aleksandar, PhD – Serbia
Slobodan Simic, PhD – Bosnia and Herzegovina
Mladjan Dragan, PhD – Serbia
Domazet Sinisa, PhD - Serbia

Design

Mladenovic Milica, PhD
Komazec Nenad, PhD

Edition

75 copies

The press:

Stamparija Donat Graf, Grocka, Belgrade

ISBN

978-86-80692-10-4

Notes:

The authors opinions expressed in this book do not necessary reflect the views of the institution in which they are employed

All papers are reviewed and checked for plagiarism

Papers which express any form of discrimination shall not be published



CONTENT

1. GEOSTRATEGIC IMPLICATIONS OF THE RUSSIAN-UKRAINIAN CONFLICT <i>Bozidar Forca</i>	17
2. CHALLENGES OF CRITICAL INFRASTRUCTURE PROTECTION IN CONTEMPORARY SECURITY ENVIRONMENT <i>Dragisa Jurisic</i>	41
3. MASS SURVEILLANCE AND PRIVATE COMPANIES <i>Sinisa Domazet</i>	48
4. REVIEW OF THE RISKS OF AUTONOMOUS WEAPONS <i>Katarina Jankovic, Nenad Komazec, Drazan Erkcic</i>	54
5. ONE APPROACH TO DETERMINING THE DANGERS TO THE SECURITY- INTELLIGENCE SYSTEM OF THE REPUBLIC OF SERBIA <i>Nenad Kovacevic, Antonio Mak, Zoran Karavidic</i>	63
6. CRITICAL INFRASTRUCTURE PROTECTION IN SOME BALKAN COUNTRIES IN COMPARISON WITH BOSNIA AND HERZEGOVINA <i>Zeljko Zoric</i>	71
7. RIGHTS AND OBLIGATIONS OF THE CITIZENS IN EMERGENCIES <i>Slajana Eric</i>	78
8. EMERGENCY HEADQUARTER'S "TABLE TOP" EXERCISES IN LOCAL GOVERNMENTS <i>Dragisa Jurisic</i>	83
9. THE POSSIBILITY OF USING AN AIRBAG AS AN ALARM FOR INJURIES AT WORK <i>Predrag Vasiljevic, Milorad Danilovic, Slavica Antonic</i>	90
10. PERSONAL DATA PROTECTION – FRAMEWORKS, PRACTICAL EXPERIENCES AND CHALLENGES <i>Radoslav Rakovic</i>	95
11. RESCUING FROM THE RUINS <i>Branko Babic</i>	106
12. COUNTERING THE THREAT OF UNMANNED AERIAL SYSTEMS TO CRITICAL INFRASTRUCTURE <i>Goran Maksimovic</i>	113
13. RISK MANAGEMENT DURING THE PANDEMIC <i>Goran Bozic, Hatidza Berisa</i>	124
14. COMPARATIVE ANALYSIS OF NATIONAL SECURITY STRATEGIES <i>Bozidar Forca</i>	132
15. TOOLS TO REDUCE VULNERABILITY FROM HYBRID THREATS <i>Tatjana Georginova</i>	144

16. LEGAL REGULATION AND CONTROL OF THE SECURITY SYSTEM OF THE REPUBLIC OF SERBIA <i>Zorana Ivetic, Jovanka Tosic</i>	152
17. CURRENT STATE OF EMERGENCY MANAGEMENT IN THE REPUBLIC OF SERBIA <i>Jovanka Tosic, Zorana Ivetic</i>	161
18. MILITARY APPLICATION OF ARTIFICIAL INTELLIGENCE <i>Milan Miljkovic, Hatidza Berisa, Srdjan Zgonjanin</i>	169
19. METHODOLOGICAL PROBLEMS OF DESIGNING RESEARCH IN SAFETY SCIENCES <i>Samed Karovic, Jovanka Tosic, Zorana Ivetic</i>	175
20. ASPECTS OF MACHINE LEARNING IN HUMANITARIAN DEMINING PROCESSES <i>Dejan Blagojevic, Gordana Jovic, Aleksandar Milic, Bojan Glamoclija</i>	184
21. ENERGY SECURITY AT THE CORPORATE LEVEL <i>Radislav Jovicic</i>	191
22. STRATEGIC MANAGEMENT IN CBRN EVENTS: APPLICATION OF WORD ASSOCIATION TEST <i>Halil İbrahim Çiçekdağı, Fatime Ökenek, Yıldız Tosun</i>	201
23. ENERGY SECURITY AS A PARADIGM OF CONTEMPORARY GEOPOLITICS <i>Srdjan Zgonjanin</i>	213
24. BEST PRACTICES IN CIVIL PROTECTION MANAGEMENT: IDENTIFYING CHALLENGES, RECOMMENDATIONS, AND INTERNATIONAL CASE STUDIES <i>Katarina Strbac, Branislav Milosavljevic</i>	222
25. MODERN ARMED CONFLICTS AND RESERVE MILITARY FORCES <i>Hatidza Berisa, Goran Korsev</i>	230
26. SYSTEMATIC APPROACH TO RESOLVING CRISIS DUE TO EPIDEMIC/PANDEMIC DISEASES <i>Slobodan Simic</i>	237
27. RIVER BASIN WATER RETENTION CAPACITY COUPLING WITH NBS FOR HYDRO-METEOROLOGICAL DISASTER RISK REDUCTION <i>Branislava Matic</i>	243
28. PERFORMING MOBING IN THE PUBLIC SECTOR <i>Leon Vedenik</i>	250
29. ANALYSIS OF COMPLIANCE OF VALJEVO DISASTER RISK ASSESSMENT WITH METHODOLOGY <i>Srecko Vukovic, Serif Bajrami, Katarina Jankovic</i>	259

30. APPLICATION OF SIMULATIONS IN TARGETING TRAINING <i>Zeljko Jokic, Aleksandar Aleksic, Marko Radovanovic.....</i>	266
31. THE ROLE OF THE SERBIAN ARMED FORCES IN THE SYSTEM OF PROTECTION AND RESCUE IN FIGHTING NATURAL DISASTERS - A CASE STUDY OF THE FLOOD OF 2014 IN THE REPUBLIC OF SERBIA <i>Serif Bajrami, Stefan Pusulic.....</i>	272
32. SIMULATIONS AND THE QUALITY OF MILITARY EDUCATION <i>Nenad Komazec, Aleksandar Milic, Aleksandar Petrovic.....</i>	278
33. FOREST FIRES AND CLIMATE CHANGES IN THE REPUBLIC OF SERBIA <i>Jelena Lazarevic, Nikola Vukojevic, Jovica Milicevic.....</i>	286
34. RESPONSE OF THE ARMY OF SERBIA TO NON-MILITARY THREAT - MIGRATION <i>Nikola Banjac, Nenad Komazec.....</i>	294
35. PERCEPTION OF CIVIL DEFENSE'S STATE IN THE REPUBLIC OF SERBIA <i>Milica Mladenovic.....</i>	305
36. THE DIBR-SAW MODEL FOR THE SELECTION OF LOCATION FOR OVERCOMING WATER BARRIER WITH DEEP DRAFT <i>Katarina Dojic, Darko Bozanic, Jovica Milicevic.....</i>	313
37. HYDROTECHNICAL AND HYDROLOGICAL CONDITIONS FOR NAVIGATION IN THE CHANNELS OF THE DANUBE-TISA-DANUBE HYDROSYSTEM <i>Milorad Tesanovic, Vladimir Matijevic, Svetislav Soskic.....</i>	320
38. WAREHOUSE OPERATIONS SIMULATION FOR SAFETY IMPROVEMENT <i>Tomaz Kramberger, Bojan Rupnik.....</i>	333
39. RISK ASSESSMENT DURING IMPLEMENTATION OF EXERCISES WITH MINE EXPLOSIVE ORDNANCE <i>Stefan Pusulic, Aleksandar Milic.....</i>	340
40. CAMOUFLAGE, CONTENT OF RESOURCE PROTECTION, FOLLOWING EXPERIENCES FROM UKRAINE'S ARMED CONFLICT <i>Aleksandar Milic, Dejan Blagojevic, Srdjan Kostic.....</i>	346
41. CHARACTERISTICS AND CONSEQUENCES OF NATURAL DISASTERS IN THE TERRITORY OF THE REPUBLIC OF SERBIA <i>Nikola Vukojevic, Stefan Tosic, Aleksandar Petrovic.....</i>	355
42. STRATEGIC DIMENSIONING OF THE DEFENSE SYSTEM OF THE REPUBLIC OF SERBIA BASED ON THE PHYSIOLOGY OF MODERN ARMED CONFLICTS <i>Katarina Jankovic, Srecko Vukovic, Slavica Dabizljevic.....</i>	363

GEOSTRATEGIC IMPLICATIONS OF THE RUSSIAN- UKRAINIAN CONFLICT

Bozidar Forca^{1a}

¹ Faculty of Business Studies and Law, University of UNION Nikola Tesla, Juriša Gagarina
141a Belgrade, Republic of Serbia, bozidar.forca@fbsp.edu.rs

Received: 17th September 2023

Accepted: 18th September 2023

Original scientific paper

Abstract: *In the history of international relations, there are evident processes in which certain events in them culminate in such a way that they are characterized as - nothing will be like before. Such a process in recent history is the Cold War, and the event is the demolition of the Berlin Wall in 1989. In combination with the tectonic disturbances created by the fall of the Berlin Wall and in the conditions in which the USA tried to establish a unipolar world order, there was a war between Russia and Ukraine in 2022, which expanded into a conflict between the collective West and Russia. It is heard again - nothing will be the same again.*

This paper is an attempt to predict the geostrategic implications of the Russian-Ukrainian conflict. The general hypothesis from which it was started is as follows: International relations are primarily state-centric, and the creation of a new world order determined by world powers is turning into a cluster arrangement of the world.. In confirming the hypothesis, well-known scientific methods were used, primarily comparative, content analysis, analogy and case studies. The general conclusion can be: The war between Russia and Ukraine, which has expanded into a conflict between the collective West and Russia, will result in a geostrategic realignment of states in the creation of a new cluster-type world order, and the possibility of the outbreak of the Third World War should not be ruled out.

Key words: *: Russian-Ukrainian conflict new world order, geostrategic implications, cluster arrangement of the world*

(introductory lecture of the forum - work by invitation)

1. INTRODUCTION

The period after the Second World War until the last decade of the last century is called the Cold War, i.e. the bipolar world order. Bipolar world order, because only two world powers - the USA and the USSR - had the greatest influence on international relations. The Cold War, because there was no direct armed conflict between the aforementioned world powers.

^a ORCID: 0000-0003-4894-3772

The Cold War ended with the victory of Western countries led by the USA, and the formal act (event) of the end of that war was the demolition of the Berlin Wall (1989), as its symbol. The fall of the Berlin Wall was followed by "tectonic disturbances", which are known as powerful disintegration processes. The most significant of these processes are: 1) the dissolution of the Warsaw Pact and 2) the collapse of the USSR, which occurred in 1991. Among the disintegration processes affecting our reality, not so much world processes, is the breakup of the SFR Yugoslavia, which began in 1991 and has not yet been completed (Forca, 2021).

The USA tried to use the newly created situation in international relations after the Cold War to create a unipolar world order, with its own dominance. For the sake of strengthening the levers of its own power, America preserved NATO, even though the Warsaw Pact fell apart. Also, the USA wholeheartedly supported the formation of the European Union (1992), as a product of the end of the Cold War, but kept it "under its control".

One of the problems that arose after the Cold War was the position of the countries of the former VU, the USSR and SFR Yugoslavia. The USA used its power and influence, and attracted most of the states from the mentioned areas to NATO, which in 2023 reached the number of 32 member states, from 12 when it was formed in 1949, or 16 at the end of the Cold War.

With the continuous expansion of NATO to the east, the Alliance broke out on the borders of Russia. Russia opposed NATO expansion, but did not have the capacity to counter it in the first decade after the Cold War. When NATO more seriously threatened to admit Georgia and Ukraine, as former republics of the USSR, into its membership, Russia strongly objected. First, in 2008, with a military intervention in Georgia, it blocked its path to NATO, and recognized its two parts (Abkhazia and South Ossetia) as independent and independent states. The matter with Ukraine was much more complicated. Russia first annexed Crimea in 2014 (returned Crimea to Russia), then in 2022 it would militarily attack Ukraine. Russia named the military intervention in Ukraine as a "special military operation", while the UN General Assembly called the act aggression.

The countries of the world reacted differently to Russia's aggression against Ukraine. The countries around the USA (the collective West) wholeheartedly sided with Ukraine, offering it all kinds of help, which is especially expressed by the delivery of weapons and military equipment. On the other hand, sanctions were introduced against Russia that were not recorded in history. A large number of countries in the world, which, like the collective West, condemned Russia's aggression against Ukraine, did not take sides, and especially did not impose sanctions on Russia.

The war in Ukraine is still going on, and relations between NATO and Russia are becoming increasingly strained. The world is threatened by the Third World War. In such conditions, the latest world order is being created, which, it seems, will not have the character of either multipolar or unipolar, but globalization will be replaced by a cluster arrangement of the world.

2. THE NEW WORLD ORDER

From a theoretical point of view, as befits discussions at a scientific meeting, it is necessary to refer to the phrase "new world order" and its characteristics in recent history. Without carrying out the methodological approach of defining the world order, we will use its dictionary-encyclopedia definition (Table 1) and the widespread definition given by Aksapar.

Aksapar defines the world order as follows:

"Every international order is a reflection of the global political and economic architecture that takes shape as circumstances allow; as such, the world order is not written or predestined, but

rather an arrangement selected from among existing options; the world order is shaped by the permanent interests and convictions of the leading actors; each new order corrects some of the shortcomings of previous orders; each world order consists of numerous competing economic, political, military global and regional orders; world orders have not been truly universal until now" (Akçapar, 2009).

Table 1. Definitions of world order (Source: Prorokovic, 2017)

DEFINITION	SOURCE
A system of controlling events in the world, and especially a set of international arrangements established to preserve global political stability.	Oxford Dictionary, 2015. www.oxforddictionaries.com
A political situation in which countries are no longer divided by their support for the US or the USSR and are instead oriented towards working together to solve international problems.	Cambridge Dictionary, 2016. http://dictionary.cambridge.org
A political, economic or social situation in the world in a certain period of time that produces consequences for relations between different countries	MacMillan Dictionary, 2015. www.macmillandictionary.com
A system for controlling world events in order to maintain political stability.	21st Century Lexicon, 2014. www.dictionary.com

Numerous examples of the typology of the world order are known in theory, and we will mention only a few. American political scientist Kaplan, in 1957, offered six models of world order: System of balance of power; Loose bipolar system (loose bipolar system); Tight bipolar system; Universal international system (universal international system); Hierarchical international system; Unit veto system (More: Kaplan, 1957).

American politician and diplomat Henry Kissinger in "World Order" (2015), sees world order as a regional or civilizational concept of the nature of a just arrangement and redistribution of power that is applicable to the entire world. Any successful world order, according to Kissinger, is based on a balance between legitimacy and power, where legitimacy is a set of generally accepted rules that define the limits of acceptable action. On the other hand, power is necessary, but not sufficient. Kissinger highlights four specific conceptions of "order": 1) the European system, especially its Westphalian model of sovereign states with equal status in the system; 2) the Islamic system based on the idea of community or community; 3) the Chinese system based on traditional ideas of the Middle Kingdom as a great center of regional power; and 4) an American system that will be dominant around the world, which is under unprecedented pressure (Kissinger, 2015).

Starting from the claim that states were and remain the key subjects of international relations, and that the world order is state-centric, numerous authors use three models in its classification: 1) unipolar, 2) bipolar and 3) multipolar world order. That classification will be key in this paper.

2.1. Bipolar world order

In theory, there is a consensus that the period after the Second World War until the last decade of the last century was essentially a bipolar world order, dominated by two world superpowers: the USA and the USSR. In conditions of bipolarity, international relations are dominated by two centers of power, two poles with opposing interests. Their total power potentials significantly deviate from the indicators of other actors. That is why the other actors individually are not able to match either of the two genders. They are forced either to join together to protect their interests, or to join one of the sexes (Prorokovic, 2018).

It is interesting to look at how the term "bipolarity" came about. Namely, the origin of that term is linked to the prominent theoretician of neorealism, Kenneth Waltz. Waltz himself says about it in an interview:

"I first published the article on the stability of the bipolar world in 1964. It was controversial. Many were enraged by my views. First, I presented it in the form of a presentation for a conference organized by Harvard and MIT. My presentation caused a lively and heated discussion. I argued that we live in a world with two forces, therefore a bipolar world. Others answered me: 'No, wait, Europe also counts'. Well, yes, of course, Europe also counts, but not as much as it was the case before and nowhere near as much as the USA and the Soviet Union. In the end, the fate of the world depended on the USA, the Soviet Union and their mutual relations" (Site: <http://globetrotter.berkeley.edu/people3/Waltz/waltz-con4.htm>).

The Cold War, as another name for the period of bipolarism in international relations, is theoretically understood in a narrower and broader sense. In a narrower sense, the Cold War is placed in the period from the end of the Second World War, until the "Cuban crisis", in 1962 (Naj, 2006; Vukadinovic, 2001). Nevertheless, the broader meaning of the duration of the Cold War, which is the most used in the literature, was given by Cagli and Witkoff, who break it down into three phases: 1) the first phase - *confrontation*, from 1945 to 1962, 2) the second phase - *from coexistence to détente*, from 1963 to 1978 and 3) the third phase - *from renewed confrontation to rapprochement*, from 1979 to 1991 (Kegley & Witkoff, 2006).

Kegley and Witkoff, in their work *World Politics - Trend and Transformation*, when it comes to the Cold War, primarily focused on the relationship between the USA and the USSR, analyzing it through the previously mentioned stages. However, the bipolar world order, or the Cold War, globally, had other general characteristics. The general characteristics of the bipolar world order include: 1) bloc grouping, 2) anti-colonialism and the creation of the Non-Aligned Movement, and 3) the arms race (Forca, 2022a).

America was the first to articulate the danger of spreading the influence of the USSR in Europe and the world after the Second World War. In this sense, in 1949, at the initiative of the USA, the Agreement on the formation of the North Atlantic Alliance - NATO was concluded in Washington. When it was formed in 1949, NATO consisted of the USA and Canada and 10 European countries. Although NATO was formed in accordance with Article 51 of the UN Charter, as a defense alliance of the North Atlantic area, the goals of its formation were "formulated" differently by its first secretary general, Lord Ismay, with the words: 1) Germany under control, 2) Russians out of Europe and 3) America to Europe (Kekovic & Dimitrijevic, 2017). Kegley and Witkoff saw in the formation of NATO, in fact, the effort of the USA to create a unipolar order, relying on its superiority in nuclear weapons and attracting Western European states to the Alliance, in order to prevent the influence of the USSR (Kegley & Witkoff, 2006). Kegley and Witkoff recognized such an effort by the USA in the "Truman Doctrine" (a strategy to contain the influence of the USSR) immediately after the Second World War. That is why the first period of the Cold War is called "confrontation". That confrontation was mitigated by the fact that the USSR very quickly produced nuclear weapons.

In the beginning, the USSR did not pay much attention to the formation of NATO, because Stalin believed that the Soviet influence in the countries of Eastern and Central Europe was strong and sufficient to oppose it. However, when West Germany was admitted to NATO (1955) and the deployment of American missiles in Turkey began, the USSR formed the Warsaw Pact in 1955 with the eight socialist countries of Europe. Like NATO, the Warsaw Pact was formed in accordance with Article 51 of the UN Charter. Thus, by 1955, two of the strongest military alliances ever made in human history were formed (Figure 1), whose armed forces numbered in the millions.



Figure 1. NATO and the Warsaw Pact in 1955

Source: <https://vk-spy.ru/bs/animals/vosstaniya-v-stranah-varshavskogo-dogovora-varshavskii-dogovor/>

With the formation of two military blocs, a strong arms race began, led by the USA and the USSR, keeping the world in constant fear of another major war. During the Cold War, the world was closest to the Third World War in 1962, in the so-called the Cuban crisis, that is, in opposing the USA that the USSR installs missile systems on the territory of Cuba. The conflict between the USA and the USSR (NATO and VU), however, did not occur, but the antagonism of the world powers was transferred to the UN Security Council, and manifested itself by vetoing the adoption of resolutions by that body. The right of veto is established in the UN Charter (UN Charter, 1945: Art. 27). Professor Adam Roberts claims that during the Cold War (until 1989) the right of veto was used 230 times: 114 times by the USSR, 67 times by the USA, 30 by the United Kingdom, 18 by France and 3 by China (Chomsky, 1993).

Although the world powers did not directly clash during the bipolarism (Cold War), nevertheless, they were the cause and participants of numerous wars of that period. In theory, there are extremely different data on the number of wars during the Cold War. Thus, according to the data of the Austrian political scientist Heinz Gertner, during the Cold War, 159 wars took place, in which more than half of the total number of countries participated (94 out of 174), and the number of wars was led by Great Britain (16 wars) and France (13 wars) as colonial powers, followed by the USA (11 wars), India (10 wars), South Africa and China (9 wars each). (Petranovic, 1990). According to another source, during the Great War, 95 wars took place (30 inter-state and 65 intra-state), and major powers participated in most of them (Delibasic et al., 2017). Similarly, the data also show that during the Cold War there were 93 wars, of which 38 (41%) were interstate, and in almost all wars the USA was involved (Jeftic et al., 2018).

Participation in two wars is characteristic of the USA and the USSR. First, the USA learned lessons from the war in Vietnam, after which there was a radical change in the way of warfare and recourse to the so-called low-intensity conflicts, with a focus on the so-called operations beyond the significant engagement of armed forces. On the other hand, the USSR became mired in a ten-year war in Afghanistan, from which it emerged in 1989, just before its collapse.

The arms race, however, produced results for one side (the US and its allies) in the Cold War. Namely, as Todor Mirkovic claims:

"The arms race between the USA and the USSR, that is, NATO and the Soviet Union, was, in essence, a race between unequal competitors. This inequality was primarily reflected in their economic power. Thus, at the end of the seventies (1977), according to data from the World Bank, the ratio of economic power, measured by gross national product, was 4.45:1 in favor of the USA and its allies, including Japan" (Mirkovic, 2007).

The USSR and the Soviet Union, therefore, lost the arms race to the USA and the Western allies, which, along with other problems within the USSR itself, but also the Soviet Union, led to the end of bipolarism, i.e. the Cold War.

2.2. A unipolar world order

Unipolarity is a term that implies the domination of world politics by one superpower. Thus, Prorokovic says; "Every issue in international relations and, therefore, international security can be influenced from one center of power." And not only on the international, but also on the national security of other countries" (Prorokovic, 2018). In theory, there are diametrically opposed views on the characteristics of the unipolar world order, and on the possibility of its establishment in practice. In principle, it is believed that "ruling the world" from a single center (a single superpower) is impossible, although there are different approaches to the efforts of hegemony to achieve this.

The progenitor of offensive structural realism, John Mearsheimer, in his work *The Tragedy of Great Power Politics*, published in 2001, presented the basics of his views, recognizable in the so-called five assumptions (principles) of John Mearsheimer. In conclusion, Mearsheimer claims: „Ultimate security can only be achieved by the most powerful state in the system" (Mearsheimer, 2001).

Joshua Goldstein argued that a unipolar world order is the most stable and therefore the most desirable. In this sense, Goldstein says: "...if one superpower concentrates as much power as possible in its hands, other actors will be less and less able to challenge its leadership." A superpower achieves preponderance of power and there are no equal competitors who could threaten it" (Goldstein, 1994).

Wohlforth William expresses very similar views on the unipolar world order to Goldsatin, who claims: "...competition in these circumstances is minimal because the dominance of one power leads to the absence of war between great powers." The other participants do not have sufficient power potential to oppose the superpower, so the confrontations that occur with the other actors are of low intensity and are mostly conducted for prestige. Simply, the power of a superpower is so great that it removes "hegemonic rivalries" due to which the importance of the balance of power on international relations decreases" (Wohlforth, 1999).

Robert Gilpin argued that hegemony in a unipolar world order excludes the balance of power ("hegemonic rivalry") and says: "...changes in structure occur due to the 'overexertion' of a superpower, as a result of which its power begins to decline." Maintaining order costs money, and every superpower faces a moment when the costs of maintaining the system become greater than the profits to be reaped. Thus, space is opened for the rise of a new hegemon that will establish a new order with its own rules of the game and new values that it will promote" (Gilpin, 1988).

The majority of analysts agree that the attempt to create a unipolar world order came after the Cold War (period of bipolarity). The USA tried to establish such an order. Namely, using the newly created situation after the dissolution of the Soviet Union and the collapse of the USSR,

America saw a chance to establish global hegemony, that is, a unipolar world order. Although the aspiration for US world domination dates back to Woodrow Wilson (Avramov, 1997) and later Harry Truman, the hegemony in the new world order was very clearly and publicly announced by the then US President George Bush (senior) in the editorial of the US National Security Strategy from In 1991, and after the war in Iraq:

"The New World Order is not a fact; it is an aspiration and an opportunity. We have an extraordinary opportunity, enjoyed for several generations, to build a new international system in accordance with our values and ideals, while old patterns and certainties crumble around us. There can be no retreat for America from the world's problems. Within the wider community of nations, we clearly see our role. We must not only protect our citizens and our interests, but also help create a new world in which our core values not only survive but flourish. We must work with others, but we must also be leaders" (National Security Strategy of the USA, 1991).

American strategists respected the views of security studies, especially those that pointed to the fact that the world cannot be ruled from one center, that is, that one power alone cannot be the world hegemon. In this sense, using the position of Russia after the collapse of the USSR and the still unconsolidated European Union, the USA, in addition to its evident economic power, also needed a strong military lever of power. In this sense, the US managed to preserve NATO, even though the Warsaw Pact fell apart. In his doctoral dissertation, Vladimir Ateljevic writes about the way in which the USA is the guardian of NATO after the Cold War:

"Although it was formed as a defense alliance, the new paradox after the end of the Cold War is that NATO appears in practice as a regional arrangement in the sense of Chapter VIII. Regardless of the opinion of one group of authors that NATO cannot be considered a regional organization in the sense of Title VIII, practice seems to refute this theoretical point of view, because UN Security Council Resolution 787 put NATO in the position of a regional organization. More precisely, there are four operations on the territory of the former Yugoslavia in which NATO is participating in terms of measures to implement the decisions of the Security Council, that is, on the basis of Article 53. These are the following operations: *Operation Maritime Monitor*, *Operation Sharp Guard* and *operations Deny Flight* and *Close Air Support* (Ateljevic, 2016).

Considering that it survived in the mentioned way, it was expected that the role of NATO would be replaced by the USA, which happened relatively quickly. The collapse of the Soviet Union and the USSR created a "buffer zone" between Russia and NATO, which consisted of European countries, former members of the Soviet Union, and newly formed states in the territory of the former USSR. (Figure 2) The introduction of these countries into its composition was first started by the EU, in 1995, when it received Austria, Sweden and Finland. However, these were militarily neutral states. NATO began its expansion in 1999 with the admission of Hungary, Poland and the Czech Republic. On the other hand, in 1999, on its 50th birthday, NATO demonstrated the power of the new world order on a half-disintegrated state, that is, it carried out aggression against FR Yugoslavia.



Figure 2. Buffer zone between NATO and Russia at the end of the Cold War

Source: Forca, 2003

The grotesqueness of the fact about the expansion of NATO to the east is all the greater if it is known that Western leaders, especially from the USA, assured the then president of the USSR Gorbachev "... that with the unification of Germany (1990) and its membership in the Alliance, NATO will not expand even an inch to the east" (Forca, 2022a).

On the 50th birthday of NATO (1999), under the strong influence of the USA, the sixth Strategic Concept of the Alliance was adopted, which will symbolize the aspiration of the USA to be a leader, as well as the new role of the Alliance. Ateljevic writes about this: "The novelty brought by this document is contained in the wording that since the fall of the Berlin Wall and the dissolution of the Warsaw Pact, NATO has not only the task of self-defense, but also of ensuring global security against terrorism, organized crime, obstacles in the flow of vital resources, and unrestricted movement large number of people, etc. (Ateljevic, 2016). Thus, NATO, unequivocally, from a defense alliance, formed in accordance with Article 51 of the UN Charter, grew into a lever of US power to rule the world. Thus, in that strategic concept from 1999, two very dangerous goals of the Alliance were determined: 1) expansion to east and 2) engagement outside the North Atlantic area, with or without the mandate of the UN Security Council (The Alliance's Strategic Concept, 1999).

The US intentions and NATO's position in their plans were completely exposed in 2001, after the Al-Qaeda terrorist attacks on facilities in New York and Washington. Clearly surprised by the way terrorists operate, US President George Bush (Junior) announced America's preemptive strategy and announced three days after the terrorist attacks, which was also written in the US National Security Strategy, 2002, and told the nation:

"Just three days away from these events, Americans do not yet have the distance of history." But our responsibility to history is already clear: to respond to these attacks and free the world from evil. They attacked us with theft, fraud and murder. This people is peaceful, but fierce when provoked to anger. The conflict began at a time and under conditions determined by others. It will end in a way, precisely on the hour, of our choosing" (National Security Strategy of the USA, 2002).

America, using NATO, really started a "fierce" response to Afghanistan, which provided shelter to Al Qaeda during the terrorist attacks in 2001. Thus, already in the autumn of the same year, the bombing of Afghanistan began, and the war in that country will last for 20 years, that is, it will end shamefully. with the withdrawal of the USA and NATO in 2021. However, the war in Afghanistan was not the only one. America and NATO began to get bogged down more and more in military interventions around the world. Thus, it was the turn of a new attack on Iraq, in 2003, which was carried out under false accusations that Iraq had weapons of mass destruction, then the war in Libya (2011), Syria (2014) and other interventions around the world.

America needed a stronger NATO to engage around the world. Therefore, after the first expansion in 1999, the Alliance expanded significantly in 2004, when it received seven new member states. Thus, in 2004, NATO grew to 26 member states, and primarily the countries of the former Warsaw Pact and the newly created states in the territory of the USSR were admitted. So, NATO was erasing the "buffer zone" with Russia. That year, in 2004, with the admission of the Baltic States, NATO broke out on the borders with Russia. The expansion of NATO was accompanied by the expansion of its ally – the European Union. However, an unwritten rule was established - *first in NATO, then in the EU* (Forca, 2021).

The idea of blocking (preventing) Russia by the USA is older than the time of the formation of NATO. Namely, that idea is contained in the works of Alfred Machen: *Expansion along the meridians* and *The Anaconda Strategy*, from the beginning of the 20th century (Figure 3).

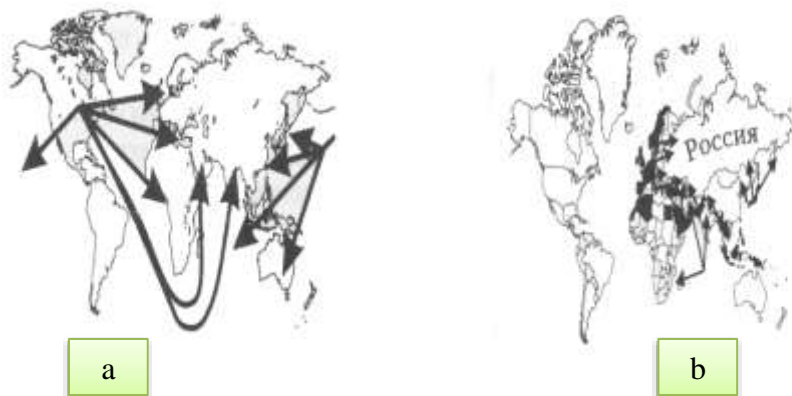


Figure 3. (a) US expansion along meridians and (b) Anaconda strategy
Source: Dugin, 2004

As far back as 1900, Mehen believed that American expansion into new areas and appropriation of new territories was a natural expansion (Figure 3a), citing as similar examples the British conquests of Gibraltar, Malta, Egypt, India, and Cyprus. In that expansion, the main threat to Mehen was Russia. Mehen designated the Pacific as a kind of "zone of responsibility" for the USA and stated that, in order to dominate the World Ocean, it would be necessary to form a whole system of naval bases (Cuba, Panama, Hawaii, the Philippines and others), in order to realize the stated goal. . The proposal for solving geopolitical problems and with the aim of achieving American national interests was formulated by Mehen in the form of the so-called "anaconda strategies" (Figure 3b). (Mehen, 1900).

Machen's theory is followed by Nicholas Spykman's theory. Spykman developed the "concept of integrated power", believing that global dominance is possible only if the "principle of combined approach to land and sea power" is applied, he concluded that "the US must achieve

its presence around the world by installing naval and air power in strategically key points of the world in order to be able to guarantee stability in the world" (Despotovic, Glisin, 2020). Thus, according to the data of Professor David Vine at the American University in Washington, the USA has around 800 bases in the world today, and the number of soldiers varies and ranges from 150,000 to 200,000 (Forca, 2022b). In this sense, after the formation of NATO, as well as using American bases in the world, the so-called pincers around Russia (Figure 4).



Figure 4. Pliers around Russia

Source: <https://www.koreni.rs/ratovi-u-sfrj-pocetak-pohoda-na-rusiju/>

2.3. Multipolar World Order and US Resistance

From a theoretical point of view, multipolar world order implies the equal influence of several (more than 2) centers of power on the totality of international relations. Prorokovic writes about this:

"This phenomenon in international politics, viewed from a realistic point of view, is described as "classification of states according to their military, economic and other war-fighting capabilities. However, multipolarity can also be understood as the ability of an actor to influence other participants in a cultural-historical, ideological-political or informational sense. The potentials of military and economic power are certainly the most important, but not the only factors that an actor can use in order to become an important pole of international relations" (Prorokovic, 2018).

The theory does not have a consistent answer to the question of a multipolar world order, which can be understood, however, in the state-centric understanding of the international system, there were and are different theories about the structure of that order. These views on multipolarity came about immediately after the collapse of the bipolar world order, i.e. at the end of the Cold War. We will mention only a few examples:

"Bergner saw Germany, Japan and the USA as the powers of the 21st century. Richard Rosecrans believes that five big centers will be able to control international relations: USA, Russia, European Union, Japan and China. Prof. Dr. Ranko Petkovic projects a kind of genesis of influence in international relations, namely: unipolarism (USA) turns into tripolarism (USA, Germany, Japan), which he believes is still present in unipolarism; tripolarism turns into pentagonalism (USA, Germany, Japan, China and Russia). Considering that in addition to the aforementioned forces on the global level, the influence of certain countries on the regional level is stronger, Prof. Dr. R. Petkovic says 'then we can be close to the conclusion that the

future of the world is in multipolarism, regardless of the forms and time of its manifestation and predominance'. Professor Muhong gives an interesting vision of future multipolarity through four triangles, which represent a square as a whole. The first triangle consists of the USA, Japan and China (the deciding factor in the Asia-Pacific region); others consist of China, the USA and Russia, but in it bilateral relations between China and Russia are the foundation; the third is composed of the USA, Japan and Europe, but in it Japan and Europe are partners subordinate to the USA; the fourth triangle consists of the USA, Russia and the European Union, in which changes are taking place. In that fourth triangle, some EU members want to break away from US influence (especially Germany and France), and Russia is a key element between the EU and the US. Prominent Indian jurist Swarup-Pathak sees the world as multipolar with the UN as the foundation of the world community, without specifically specifying the centers of power. Swiss experts in the field of international relations, Rphilippe Braillard and Mohammad-Reza Djali, have a similar opinion, who say: '*...The bipolar structure of the world has been replaced by an extremely complicated system, but without reference points*' (Forca, 2003).

Acclaimed theoretician Joseph Nye is of the opinion that not only states are influential factors influencing the creation of a multipolar world order, but that there are also other "dispersers of power". In this sense, Nye, about the world order after the Great War, writes:

""The bipolar world no longer exists, but it will not be replaced by a unipolar world empire controlled by the US alone. The world, from an economic point of view, is already multipolar, and as the information revolution progresses and interdependence increases, and transnational actors on the international stage become more and more important, there will be a dispersion of power. The new world will not be perfectly ordered and you will live with it" (Nay, 2006).

Observing the world from a state-centric point of view, most theorists agree that the multipolar world order in official documents and in their practice was first advocated by Russia and China, in the first and second decades of this century. In this sense, there is talk of three world powers, to which the European Union is added in some works, but until the ugly conflict between Russia and Ukraine in 2022. Namely, since then numerous analyzes point out that the EU has fallen under the complete domination of the USA and NATO.

Trying to point out the perniciousness of unipolarity in international relations, in February 2007, in an address at the conference on international security in Munich, Russian President Putin "presented a series of criticisms against the existing form of international relations, labeling the USA as the main "culprit" of excessive the use of force in international relations and the overstepping of one's own borders, which produced a global sense of insecurity and stimulated an arms race. In addition, Putin noted that the sum of the GDP of India and China is already higher than the GDP of the United States, as well as that a similar calculation of the GDP of the BRIC countries (Brazil, Russia, India and China) exceeds the cumulative GDP of the European Union" (Website: <https://www.youtube.com/watch?v=hQ58Yv6kP44>, 11.09.2023).

In his speech from 2007, Putin presented the positions of Russian foreign policy in relation to the USA, arguing against the unipolar international order, and therefore the global dominance of the United States. Putin also announced that the multipolar international order has already taken hold, thereby indicating that the unipolar order is a thing of the past. In challenging the legitimacy of the international order, Putin managed to secure the support of a significant number of countries, the most significant of which was certainly the one that came from the People's Republic of China. Along with the diplomatic offensive to ensure the support of the great powers, Russia made enormous diplomatic efforts to emphasize the importance of existing international organizations, especially the United Nations and the OSCE, due to the

unique legitimacy these organizations have in the international framework, and especially due to the fact that in them Russia is an indispensable subject in the decision-making process (Obradovic, 2021).

The USA and its allies did not pay too much attention to the views of President Putin, in which sense the expansion of NATO continued, and in 2008, at the summit in Bucharest, an invitation was sent to Georgia and Ukraine to join the Alliance. In such conditions, using inter-national antagonisms in Georgia, Russia militarily attacked that country in 2008 and after a short war recognized its parts Abkhazia and South Ossetia as independent and independent states. Such a move by Russia was met with indignation by the USA and Western countries. However, President Russia did not refer to that fact. Thus, already in 2009, Russia adopted the first National Security Strategy, in which the international order was assessed as multipolar, and the USA and NATO were identified as the key security threats (Strategy of National Security of the Russian Federation until 2020, 2009). Another significant geostrategic move made by Russia is the formation of a political-economic organization known by the acronym BRICS, which refers to five countries: Brazil (B), Russia (R), India (I), China (K) and the Republic of South Africa (S). BRICS was formed in 2008, covers about 30% of the surface of the planet Earth, three billion people live on the territory of the countries that make up that organization, which is over 42% of the world's population. The gross national income (GNI) of the BRICS member states is estimated at over 16 trillion US dollars, which is over 22% of the total world GNI. (Tesanovic, 2018).

America and NATO paid less attention to Russia's moves, and became more and more mired in wars, primarily in Libya (2011) and Syria (2014), along with the already existing conflicts in Iraq and Afghanistan. However, with its strategy, Russia has announced a more significant involvement in mutual relations, which is shown by its direct participation in the war in Syria, about which Trapara writes:

"Sooner or later, Russia had to start projecting power beyond its immediate environment, especially in a strategically important (primarily due to maritime routes and energy) area such as the Middle East." For her, the Middle East in the geographical sense was actually always the "Middle South" and one of the arenas of confrontation with other great powers, so it was only a matter of time when the "great game" that Russia started in the 19th century with the Great Britain, and later continued with the USA. Putin was certainly aware of this when, after coming to power, he closed the Soviet naval bases in Vietnam and Cuba, but not in Syria" (Trapara, 2020).

After the US again invited Georgia and Ukraine to join the Alliance, in 2014 Russia returned Crimea to its composition, which the West characterized as an illegitimate annexation of part of Ukraine's territory. Also, Russia supported the resistance of the pro-Russian population in the southeast of Ukraine, which opposed the regime in Kiev. That situation influenced a stronger tightening of relations between the USA (the West) and Russia, which will be discussed in more detail in the next question.

China avoided the Cold War conflicts between the USA and the USSR and built its economy and economic influence in the world with great strides. China's strongest economic surge at the global level has been occurring since 2013, when Vice President Xi Jinping announced the "Belt and Road" Initiative (New Silk Road). China avoided entering into military integrations such as NATO, VU and the like, and instead built its influence on economic strength. However, from a regional point of view, China has made it known that its interests in the South China Sea, especially around the island of Taiwan, cannot be threatened. Also, China advocated for a multipolar world order, which is why it came under attack from the US (Forca, 2019).

The American response arrived very quickly. In the National Security Strategy from 2017, the USA identified Russia and China as revisionist states and key security threats (National Security Strategy, 2017). In this sense, the homogenization of the West began against those two countries, as two key opponents. Russia was marked as a security problem, and China as an economic opponent.

At the NATO summits, especially since 2016, from which a special declaration is issued, the development of the Defense in 3600 program began, which essentially means the already established encirclement of Russia. In the Declaration from the 2018 NATO summit, on the Defense in 3600 program, it is stated:

„Planned, the defense in 3600 includes: 1) strengthening in the north-east: the formation of four battalion-strength combat groups, about 4,500 soldiers, and their deployment in Estonia, Latvia, Lithuania and Poland, 2) the Black Sea region - multinational training brigades in Romania, 3) strengthening of national capacities and cooperation of NATO with partners in the South, 4) formation of a center for cyber warfare in Belgium, 5) maintenance of nuclear forces (members that have them: the USA, France and the UK) at the level of deterrence, i.e. depending on how this is respected by the other side - Russia (START program), 6) warning Russia not to respect the Vienna Convention on Conventional Arms Control, and the position that NATO will manage to maintain balance in that area as well, 7) with the total forces they provide for NATO, the allies will (item 14: "4×30") additionally provide: 30 naval units, 30 so-called heavy battalions of the ground army and 30 aviation squadrons, with readiness for use within 30 days or less and 8) special measures for more operational use of NATO forces: (a) provide by the end of 2019 permits for non-NATO members to quickly cross the border (land, sea, air), (b) by the end of 2018, determine the basic and alternative routes of supply and transport and (c) intensify training activities. On the other hand, the NATO "ballistic military defense" - BMD, which is operational around Russia, is interpreted as a barrier against intercontinental missiles from other areas, and not as a threat to Russia, which the Russian side does not trust" (Forca, 2020).

Against China, the USA introduced a real economic war, which it also demanded from its allies, especially in Europe. In such conditions, Russia's armed attack on Ukraine took place in 2022.

3. RUSSIAN-UKRAINIAN CONFLICT

The beginning of the war between Russia and Ukraine in 2022 was preceded by the period since Ukraine became an independent and independent state (1991), which in theory is called the "Ukrainian crisis". From a geopolitical point of view, the position of Ukraine after gaining independence can be understood in the Theory of Regional Security Complexes - TRBK, developed by the Copenhagen School of Security at the end and after the Cold War. The original creator of TRBK is Professor Barry Buzan and his work from 1983 - *People, States and Fear: The National Security Problem in International Relations*, which was continued together with Ole Weaver (Waever Ole), in 1988, in the *Work - Security: A New Framework for Analysis*, boulder, and completed in 2003 in the part - *Regions and Powers: The Structure of International Security*. In the aforementioned works, the professors of the Copenhagen School divided the world into nine RBCs, among which, according to this paper, the European and Post-Soviet RBCs stand out (Figure 5).

Although, according to Buzan, Ukraine is entering the post-Soviet regional security complex (RBK), that country still played the role of an *insulator*. The state, in the status of an *insulator*, is located between at least two regional security complexes (RBK) and separates their security

dynamics, that is, it is in a position to draw or exchange the energy of those RBK. A typical example of an insulator state is Turkey, which is located between three RBKs.

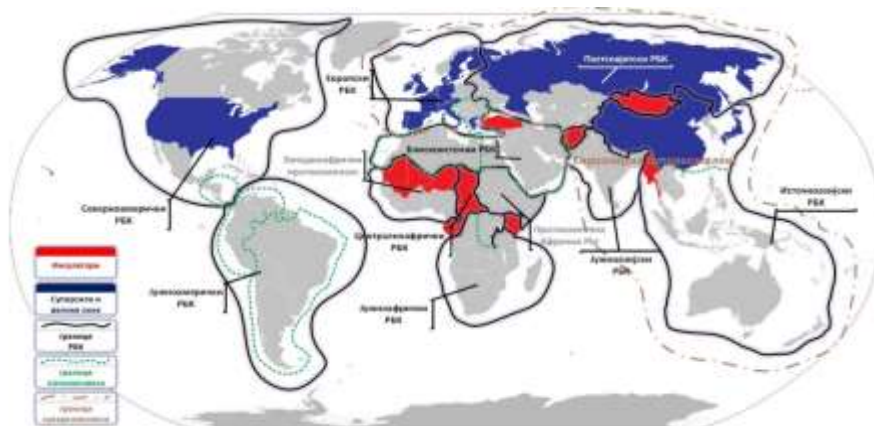


Figure 5. Regional security complexes after the Cold War
Source: Barry and Weaver (2003), in Lipovac V. Milan, 2016

In its development as an independent and independent state, Ukraine oscillated between Russia and the West (NATO and the EU), depending on which political group was in power. During the pro-Russian regime, Ukraine even passed the *Law on Military Neutrality*. On the other hand, pro-Western governments wholeheartedly pushed for membership in the EU and NATO. In this sense: "The Ukrainian crisis developed on the issue of a series of contradictions, the identity and geopolitical position of the south-eastern pro-Russian and on the other hand the north-western regions of the country, where after the Orange Revolution in 2004, the dissolution of Yanukovich's government in 2007, and the putsch on the street in February 2014, the crisis is occurring parliamentarism and pluralism, rebellions and dissatisfaction in the Southeast, which, with the interference of foreign factors, the suppression of democratic freedoms in the country and the opening of the religious problem, deepened into an unfinished conflict until today" (Petrovic & Bukvic, 2019).

After Russia returned Crimea to its composition in 2014, the areas of Ukraine with a majority Russian population in the southeast, Donetsk and Luhansk, tried to follow the same path. In those parts, riots broke out leading to armed conflicts, due to the attitude of the Ukrainian authorities towards the pro-Russian population. Russia sided with the population in Luhansk and Donetsk. The European powers Germany and France intervened in the resolution of the conflict, so that two armistice agreements, known as the Minsk Agreements from 2014 and 2015, were concluded. However, it will be shown that the Minsk Agreements, as former German Chancellor Angela Merkel says, as a participant in them, were essentially "buying time for Ukraine, because it was clear that that country could not stand up to Russia" (Website: https://www.vostok.rs/index.php?option=btg_novosti&catnovosti=2&idnovost=139188&RT:-Sporazumi-iz-Minska-dali-Ukrajini-vreme-da-postane-jaca---Merkelova). Thus, in the period 2014-2022, Ukraine continued its persecution and terror against the pro-Russian population in Luhansk and Donetsk, during which time it is believed that around 14,000 people were killed and countless of them were forced to emigrate from the country. On the other hand, Ukraine began to strongly establish its position on the lines reached in Luhansk and Donetsk, in which the Western countries were complicit. Also, NATO member countries have taken care of the training of the Ukrainian armed forces. Ukraine was preparing for war against Russia.

In addition to supporting the pro-Russian forces in Ukraine, Russia warned the authorities in Kiev that they will not tolerate their attitude towards the population of Lugansk and Donetsk, while providing the international community with information about the situation and processes in the southeast of Ukraine. The US and Western countries did not attach much importance to the Russian information, except that they continued to support Ukraine with constant calls for admission to NATO. Ukraine received the last invitation to join NATO after the US and NATO left Afghanistan in 2021. Russia did not approve of that call for Ukraine to join the Alliance, and at the end of 2021, it proposed to America and NATO a new security structure in Europe (Table 2).

Table 2. Russian proposal from 17.12.2021

(Source: <https://www.sektorbezbednosti.com/osvrt-na-nove-ruske-predloge-ugovora-o-bezbednosnim-garancijama-sa-sad-i-merama-za-jacanje-bezbednosti-sa-nato-od-17-decembra-2021-godine/>)

No-divided of Security	No nuclear war	Land-based missiles	Non-expansion of NATO to the east
<p>-which is why the security interests of all parties must be taken into account,</p> <p>- the parties will refrain from deploying troops and weapons, warships or overflights heavy bombers outside their national territories, in areas where their deploying and acting can be seen by the other party as a threat or from which they can attack the other side,</p> <p>-NATO will not conduct any military activities in the territories surrounding Russia – in Ukraine and Eastern Europe, in the South Caucasus and Central Asia.</p>	<p>-therefore, it is necessary to strengthen measures to prevent any conflict between the parties, in particular avoiding incidents at sea and in the air,</p> <p>- create additional or improve existing cooperation mechanisms,</p> <p>-refrain from conducting military activities involving use scenarios of nuclear weapons - training or exercises - with non-nuclear states armament and - refrain from training or exercising military and civilian personnel of non-nuclear states to use nuclear weapons.</p>	<p>-parties would not deploy medium- and short-range land-based missiles outside their own national territories, as well as in the areas of their national territories from which they cantarget the territory of the other contracting party/parties,</p> <p>-parties will refrain from deploying nuclear weapons outside their national borders territory, and all such already deployed weapons will be returned to the foreign owner in at the moment of entry into force of the Agreement on Security Guarantees, while the existing one will infrastructure for deploying such weapons outside their national territories be destroyed.</p>	<p>- The USA undertakes to prevent and block the further expansion of NATO to former countries members of the USSR, that they will not establish military bases on the territories of these states that are not NATO members, use their infrastructure for any military activities or develop bilateral military cooperation with them,</p> <p>-NATO member states undertake to refrain from further expansion of NATO to The East, including Ukraine and the old NATO member states (which were in May 1997.years before the first decision on enlargement and the NATO-Russia agreement) that they will not deploy additional armed forces and armaments on the territories of the new member states.</p>

Given that the USA and NATO did not respond to Russian proposals, the preventive deployment of Russian armed forces around Ukraine began and war was certain. After unsuccessful attempts in negotiations with the USA and NATO to redefine the security of Europe, especially to stop the expansion of NATO to the east and the positions of the Alliance to return to 1998, in January, Russia recognized the Lugansk People's Republic and the Donetsk People's Republic as independent states. Such a move by Russia can be interpreted in

accordance with Article 51 of the UN Charter, as the right of states to self-defense by association. In this sense, on February 24, 2022, Russia militarily attacked Ukraine, calling it a "special military operation". The term "aggression" was used by the UN General Assembly in its resolution, after Russia's military intervention.

Russia's aggression against Ukraine is still ongoing and there is no end in sight. In addition to the human losses and enormous material destruction to which Ukraine is exposed, Russia annexed four regions of that country after a referendum (September 23-27, 2022) during the war, namely: the Lugansk People's Republic, the Donetsk People's Republic, the Zaporozhye Region and Kherson region. In addition (Figure 6) to the fact that about 20% of the territory, with about 15% of the population, is outside its control, Ukraine also faced a mass exodus of the population, mainly to EU countries. It is estimated that around 10 million residents of Ukraine have left the country so far.



Figure 6. Territory of Ukraine appropriated by Russia

Source: mondo.rs/Info/Svet/a1695254/Koji-deo-ukrajinske-teritorije-je-prisvojila-Rusija.html

The reaction of the USA and Western countries, primarily the EU and NATO, could be said to have been expected. The collective West wholeheartedly sided with Ukraine, providing it with all-out support in extraordinarily large financial donations, measured in tens of billions of dollars, as well as massive military aid. On the other hand, almost all contacts with Russia were cut off, and unprecedented sanctions were introduced. According to numerous analysts, Russia's attack on Ukraine homogenized the collective West, which was shaken, especially after the shameful exit from Afghanistan in 2021. Also, numerous analysts agree that a hybrid war of the collective West against Russia is underway, as well as the creation of the latest world order.

4. STRATEGIC IMPLICATIONS

The basic question in the current geopolitical conditions after the outbreak of the war in Ukraine is - *where does it all lead and what are the geostrategic implications of that conflict?* Given that the war in Ukraine is multidisciplinary, the answers to the above questions can best be sought in the geostrategic determinations of the main actors of the Russian-Ukrainian conflict, that is, in their security strategies.

Russia adopted its last (third in a row) national security strategy before the start of the conflict in Ukraine, i.e. in 2021 (STRATEGY of national security to the Russian Federation, 2021). In

that strategy, Russia's attitude towards international relations and security is very clear. International relations are multipolar, and the main threat to security is the USA and the expansion of NATO to the east. When it comes to the conflict in Ukraine, President Putin at the beginning of the "special military operation" determined its goals: the de-nazification and demilitarization of Ukraine, while solving the issue of the Dombas region in accordance with the Minsk agreements. It is difficult to explicitly answer the question of what the denazification and demilitarization of Ukraine means, but it is likely that it implies the destruction of pro-fascist forces and not allowing Ukraine to become a member of the Alliance. As for the Dombas region (Lugansk and Donetsk), the situation on the ground has changed, that is, the Minsk agreements have been abandoned, and Dombas has been annexed to Russia.

In principle, the Russian strategy has several goals: to punish Ukraine for decades of behavior towards Russia and the pro-Russian population in Ukraine; do not allow Ukraine to become a member of NATO; to prevent the expansion of NATO to the east, and to position ourselves as favorably as possible in the latest world order that is being created.

In the past year and a half, the collective West has brought important strategic documents, among which stand out (in order of adoption): Strategic Compass for Security and Defense of the EU (March, 2022), NATO Strategic Concept (June, 2022) and the US National Security Strategy (October, 2022). An insight into all three documents unequivocally depicts the situation that the collective West, primarily the EU and NATO, fully obeys the interests of the USA.

The European Union welcomed Russia's aggression against Ukraine completely unprepared. The moves of the Union were initiated by the decisions and interests of the USA. The strategic concept of security and defense is just an attempt for the Union to restore the importance of the Common Security and Defense Policy, as part of the Common Foreign and Security Policy established in the Lisbon Treaty in 2007 (see: Lisbon Treaty, 2007).

NATO is unequivocally a lever of US power, which has been proven in over four decades of its existence, especially after the Cold War. The strategic concept of NATO (eighth in order) adopted in June 2022 is, in essence, support for the interests of the USA. In 2023, NATO received Finland and Sweden and thus grew to 32 member states, i.e. exactly 100% compared to the end of the Cold War (Figure 7).

What is not written in the Alliance's Strategic Concept, but what is realized in practice, is the creation of *a new center of gravity of the Alliance in Europe* (the Eastern wing of NATO). That center will be Poland with the so-called countries. Bucharest group (B9)^b, plus Finland and Sweden. This is indicated by at least two facts. First, apart from Ukraine, Russia has the strongest antagonisms with Poland. This fact is primarily based on the historical facts of the relationship between Poland and Russia in the centuries-old history of existence. Another fact is the enormous military strengthening of Poland, in the sense of the doubling of military personnel (numerical status) and very large expenditures for equipment and modernization in the next decade, which is expressed in the projected 110 billion euros. Thus, practically, NATO is turning the former "buffer zone" with Russia, which was part of the VU, into the so-called *eastern bulwark of the Alliance ("American Wall") towards Russia*, but also China, in modern

^b After Russia annexed Crimea in 2014, at the initiative of Romania and Poland, nine countries of Central and Eastern Europe gathered, all of which are members of NATO, and which formed their formal alliance in 2015 in Bucharest (Romania), hence the name "Bucharest Nine" - B9. These countries are: Estonia, Latvia, Lithuania, Poland, Czech Republic, Slovakia, Hungary, Romania and Bulgaria.

conditions. It is, at the same time, the American response to the Berlin-Paris axis, which was trying to get out from under US control.



Figure 7. NATO in 2023

Source: <https://hcz-zu.hr/evolucija-ruske-strategije-prema-ukrajini/>

The last US national security strategy was adopted at the end of October 2022. It is a timely continuity with the previous strategy in terms of identifying two key adversaries - Russia and China, with stronger assessments of the hostility between them and the steps that will be taken to, as President Biden claims: Contain Russia and overcome China. (National Security Strategy, 2022). It is a very indicative fact that in all three strategic documents of the collective West, the positions on Russia and China are given almost identically. This is proof that these documents were "dictated" from the same center - from Washington.

The big enigma remains China. In the strategic documents of the collective West, China is marked as an adversary along with Russia, which is given greater importance. Namely, it is claimed that only China has the strength (power) to influence the design of the latest world order. In this sense, numerous analysts point out that "after Russia, it is China's turn". Is it a bill without an innkeeper? The West is aware of China's strength and its inability to quickly resolve the conflict in Ukraine. In this sense, the documents of the collective West even foresee the possibility of cooperation with China, while for Russia that option is completely excluded.

China is aware of its strength, primarily economic. However, she is also aware of the efforts made by the West, primarily the US, to suppress the "Belt and Road" initiative, especially in Europe. According to some analysts, the Belt and Road Initiative is "dead" in Europe. China condemned Russia's military intervention in Ukraine as a matter of principle, respects the territorial integrity of states and advocates international law. But China is of the opinion that "not all the mistakes" are on the Russian side, and it directs criticism at the USA and some Western countries. In this sense, China did not impose sanctions on Russia, even more so with that country and strengthens the concluded strategic partnership and joint activities within the framework of the integrations to which both countries belong, especially BRICS and the SCO (Shanghai Cooperation Organization).

4.1. The latest world order

The general geostrategic consequence of the Russian-Ukrainian conflict, or the conflict of the collective West against Russia, will be the creation of a latest world order, or the world will

enter World War III. In the latest order, the great powers will, first of all, try to realize their interests, and other countries will adapt according to their own capabilities.

The latest world order will be neither unipolar, nor bipolar, nor multipolar. It will be the arrangement of relations between cluster-type states. Therefore, globalization is giving way to the cluster arrangement of the world. The following facts, found in documents and actions of world powers and other states, point to such a conclusion.

Clusters is a term that originated in economics, and is also used in other spheres. Thus, the well-known Porter says: "Under a cluster we mean a group of industries and organizations that are connected in buying and selling relationships or that share the same infrastructure, clients or skill base and whose connections improve the competitive advantage of the participants" (Forca, 2023b)! Clusters are best understood if we consider them as regional systems. Translated to international relations, clusters are groups of states that are connected by common interests and act as such on the international scene. Clusters are similar to regional security complexes - RBK, as seen by the Copenhagen School of Security and its famous professors Barry Bazan, Ole Vive Jaap Del Vide, Lene Hansen and others. However, the basic difference between clusters and RBK is that some common interest prevails in clusters, while in RBK that interest is not primary, but some common characteristics of (geo)space.

The strategic decisions and moves of the world powers, especially the USA, China and Russia, but also the European Union, point to the conclusion about the cluster organization of the latest world order.

The USA managed to assert itself again and more strongly as the leader of the collective West. However, the need for America to strengthen its position by creating numerous alliances (clusters) of states is felt even more clearly. The USA put the EU under full control, brought NATO to the forefront and managed to expand it to two new members - Finland and Sweden. NATO remains a strong counterweight to Russia in Europe. However, the key rival of the US, as stated in the 2022 US National Security Strategy, is not Russia but China. Therefore, the motto of that strategy is: "Contain Russia and overcome China".

In addition to NATO and the EU, the USA strongly relies on and emphasizes the importance of new and old alliances, of which the following stand out in particular:

- Group of the seven most developed countries in the world - G7: USA, Great Britain, Canada, France, Germany, Italy and Japan;

- Five

Eyes: Canada, Great Britain, New Zealand, Australia and the USA. The admission of Japan to this organization is also expected;

- Quad: USA, India, Japan and Australia;

- Aukus: USA, Australia and Great Britain. There is an initiative to expand this alliance to Japan and South Korea (Aukus+);

- I2+U2: India and Israel + USA and UAE i

- C5+1: Kazakhstan, Kyrgyzstan, Uzbekistan, Tajikistan and Turkmenistan + USA.

China and Russia, together and separately, also pay great attention to the formation and development of alliances with other countries.

China is strategically reoriented not to enter into military alliances, but to enter into integrations, primarily in the economic sphere, which also have a security aspect. In this sense, the following stand out in particular:

- Shanghai Cooperation Organization (SCO), to which Iran will join in 2022 and which now consists of: China, Russia, Iran, India, Pakistan, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan. The total territory of the SCO member countries is more than 35 million km², or 65% of the territory of Eurasia. The total population of the SCO countries (2022) is about 3.5 billion people. The organization's main tasks are strengthening stability and security in the wider area, uniting participating states, fighting terrorism, separatism, extremism, drug trafficking, developing economic cooperation, energy partnership, scientific and cultural interaction (Forca, 2021).

- BRICS, which is gaining more and more prestige among the countries of South America, Asia and Africa. After the BRICS summit in South Africa in August of this year, six countries were invited to join: Saudi Arabia, Iran, Egypt, Ethiopia, Argentina and the United Arab Emirates. According to some data, more than 40 countries of the world expect to become BRICS members, while 23 of them have submitted an official request for membership (Site: <https://www.slobodnaevropa.org/a/samit-briks-saradnja-johanesburg/32565107.html>).

- RCEP: The Regional Comprehensive Economic Partnership consists of 10 Southeast Asian countries, as well as South Korea, China, Japan, Australia and New Zealand, which was signed by 15 countries on November 15, 2020 and

- China + 17: Part of the Belt and Road initiative, which China is developing with 17 European countries, regardless of whether they are EU members or not.

In addition, China exerts an extremely strong influence in the area of Africa and some South American countries (a strategic partnership was signed with Venezuela).

Russia, in addition to its membership in the SCO and BRICS, is particularly engaged in strengthening:

- Organizations of collective security agreements - CSTO, as a security organization that is a pan-NATO and which, in addition to Russia, consists of: Belarus, Armenia, Kazakhstan, Kyrgyzstan and Tajikistan (Forca, 2021).

- Eurasian Economic Union, which includes Russia: Belarus, Kazakhstan, Kyrgyzstan and Armenia.

Like China, Russia has a growing influence in Africa and, in particular, within the group of oil producing countries OPEC, which is also named as OPEC PLUS.

A possible geostrategic consequence of the Russian-Ukrainian war is World War III, which some analysts say is already underway. However, that war, if it starts with a more direct armed conflict between Russia and NATO, cannot go without the use of nuclear weapons. **In the conditions of the use of nuclear weapons, any analysis is meaningless.**

5. CONCLUSION

War has no goal, but it has a function! Historically speaking, big wars started when some of the world powers were dissatisfied with the distribution of power in international relations, and their outcome was the creation of a new world order.

In recent history, world orders are recognizable in the alternation of their three forms: bipolarism, unipolarism and multipolarism. These forms are primarily determined by the relationship between world powers and their influence on global international relations. Since

the First World War, and especially the Second World War, two superpowers have stood out in international relations: the USA and the USSR, later Russia. In the 21st century, China is unequivocally joining those forces, primarily in the economic sense. Although some analysts are of the opinion that the European Union should be counted among world powers, nevertheless, the state and processes in the Union point to the fact of its disunity and the excessive influence of the USA.

The United States has had the greatest influence on processes in international relations in recent history. America, therefore, tried to establish a unipolar world order, preserving NATO as a lever of power, force in international relations and influencing other countries with its overall power. For some time after the collapse of the USSR, Russia was excluded from the main world events. However, since the first decade of this century, Russia has returned to the ranks of world powers, precisely through military power and the war in Georgia. China, with its economic power and influence, has unequivocally intervened among the world powers. Thus, in the state-centric system, the USA tried to maintain dominance, while China and Russia extended the multipolar order.

For the sake of preserving their own hegemony, the USA and NATO got too bogged down in war conflicts, from which they did not realize profits. It was obvious that one of the rivals (China or Russia, or both) had to be eliminated. In this sense, the USA "lit the fuse" - Ukraine, on the "line of fire" with Russia. It was not difficult, if you take into account the historical relations between Russia and Ukraine. China is "left for later".

Russia "fell" on the American trap and militarily attacked Ukraine. With this act, Russia seeks to: punish Ukraine for its attitude towards Russia, but also the pro-Russian population in its country; to prevent Ukraine from joining NATO; to stop the expansion of NATO to the east and to position itself as best as possible in the latest world order that is being created.

America profited from Russia's attack on Ukraine, because it homogenized the collective West, but not only in supporting Ukraine, but in strengthening its shaky position. The European Union unprepared for the Russian-Ukrainian conflict and completely fell under the influence of the USA. China avoided conflict in the Cold War, and now tries to remain neutral. However, since the USA and the collective West have marked China as a key opponent, that country is trying to eliminate the influence of the West and create the most favorable position for itself.

The Russian-Ukrainian conflict, which has turned into a conflict between the West and Russia, is still going on and there is no end in sight. Obviously, the only one that will lose in that conflict is Ukraine, and the question is whether and in what form it will survive. From a geostrategic point of view, the Russian-Ukrainian conflict will produce the creation of the latest world order. That order will be neither unipolar, nor bipolar, nor multipolar. All parties, especially the world powers, are creating cluster-alliances, and the latest world order will leave globalization and adopt a cluster type of relationship.

The Russian-Ukrainian conflict could turn into World War III. If that happens, it is inevitable that nuclear weapons will be used. In the conditions of the use of nuclear weapons, any analysis is meaningless.

REFERENCES

A Strategic Compass for Security and Defense of EU (2022), https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en, 15.09.2023.

Ақсапар, Б., (2009), The Mutual Existence of Nascent and Senescent World Orders, Portland State University, Occasional Papers Series, Vol. 1, No. 1, 2009.

- Ateljevic, V., (2016), Medjunarodno organizovanje i bezbednosna institucionalizacija Evropske unije, Doktorska disertacija, Fakultet politickih nauka, Beograd.
- Avramov, S., (1997), Postherojski rat zapada protiv Jugoslavije, IDI, Veternik.
- Buzan, B., (1983), People, States and Fear: The National Security Problem in International Relations, Chapel Hill: The University of North Carolina Press.
- Buzan, B., Waever, O., Wilde, J., (1998), Security: A New Framework for Analysis, Boulder, CO: Lynne Rienner.
- Buzan, B., Wæver, O., (2003), Regions and Powers: The Structure of International Security, Cambridge University Press, Cambridge.
- Chomsky, N., (1993), World Order and Its Rules: Variations on some Themes, Journal of Law and Society, Vol. 20, No. 2, Summer.
- Delibasic, D., Talijan, M., Jevtic, D., (2017), Fizionomija savremenih oruzanih sukoba kroz prizmu oruzanog sukoba u Ukrajini, Vojno delo br. 1/2017.
- Despotovic, Lj., Glisin, V., (2020); „Americka militarizacija Evrope na pocetku 21. veka kao maligna eksplikacija kontinuiteta anglosaksonskih geopolitickih doktrina”, Politika nacionalne bezbednosti, Godina XI, vol. 19, broj 2/2020.
- Dugin, A., (2004), Osnovi geopolitike, knjiga I. Zrenjanin: Ekopres.
- Forca, B., (2019), Pojas i put kao oblik ispoljavanja pametne moci Kine, Diplomacija i bezbednost, God. II, Vol. 2, br. 2/2019.
- Forca, B., Obrana u 360⁰ i stepenasti odgovor, <https://odbranaibezbednost.rs/2020/04/09/odbrana-u-3600-i-stepenasti-odgovor/>, 10.09.2023
- Forca, B., (2021), Sistemi bezbednosti, Udzbenik, Fakultet za poslovne studije i pravo, Beograd.
- Forca, B., (2022a), Savremene teorije bezbednosti, Udzbenik, Fakultet za poslovne studije i pravo, Beograd.
- Forca, B., (2022b), Smisao i ciljevi sirenja NATO na istok, Bezbednosni forum, Beograd, br. 2/2022.
- Forca, B., (2023b), Klstersko uredjenje sveta i Zapadni Balkan: <https://odbranaibezbednost.rs/2022/12/16/klstersko-uredjenje-sveta-i-zapadni-balkan/>, 03.06.2023.
- Forca, B., (2003); Vojni faktor medjunarodnih odnosa i njegov uticaj na razvoj Vojske Jugoslavije, Doktorska disertacija, Vojna akademija, Beograd. Gilpin, R., (1988), „The Theory of Hegemonic War“, Journal of Interdisciplinary History, 18, 4, 1988.
- Goldstein, J. S., (1994), International Relations, Harper Collins College Publishers, New York.
- Intervju Keneta Volca „Conversations with History“, Institute of International Studies, UC Berkeley. Dostupno na: <http://globetrotter.berkeley.edu/people3/Waltz/waltz-con4.htm>, 14.07.2023.
- Jeftic, Z., Misev, G., Obradovic, Z., Stanojevic, P., (2018), Savremeni konflikti i njihove tendencije, Vojno delo, Beograd, 7/2018., strana 23-40.
- Kaplan, M., (1957), System and Process in International Politics, New York: John Wiley and Sons.

- KisindZer, H., Svetski poredak, Klub plus, Beograd, 2015.
- Kekovic, Z., Dimitrijevic, I., (2017), Sistemi bezbednosti sa sistemom nacionalne bezbednosti Republike Srbije, Fakultet bezbednosti, Beograd.
- Kegli V. C., Vitkof R. J., (2006), Svetska politika – Trend i transformacija. Beograd: Prometej.
- Lipovac, M., (2016), Nacionalna bezbednost Republike Srbije u bezbednosnom kompleksu Zapadni Balkan, Doktorska disertacija, Fakultet bezbednosti, Beograd.
- Lisabonski ugovor, (2007), <https://www.mei.gov.rs/srl/vesti/1914/detaljnije/w/0/konsolidovana-verzija-ugovora-o-eu-i-ugovora-o-funkcionisanju-eu-dostupna-i-na-srpskom-jeziku/>, 10.09.2023.
- Mahan, A.T., (1900), The Problem of Asia and Its Effect upon International Policies, Little Brown, Boston.
- Mearshaimer, J., (2001), The Tradey od Great Power Politics, Norton, New York.
- Mirkovic, T.,(2007), NaoruZavanje i razvoj, Evropski centar za mir i razvoj (ECPD), Beograd.
- National Security Strategy of the USA (1991), The White House, August 1, 1991, Washington, Preface.
- National Security Strategy of the USA, (2002), The White House, The Washington.
- National Security Strategy of the USA (2017), The White House, The Washington.
- National Security Strategy of the USA (2022), The White House, The Washington.
- NATO Strategic Concept (2022), Madrid.
- Naj, S.DZ., (2006), Kako razumeti medjunarodne sukobe, Stubovi kulture, Beograd.
- Obradovic, Z., (2021), Geopoliticko pozicioniranje Rusije nakon intervencije u Siriji, Doktorska disertacija, Fakultet bezbednosti, Beograd.
- Petrovic, D., Bukvic, R., (2019), Ukrajinska kriza 2013-2019, IMPP, Beograd.
- Petranovic, B., (1990), Istorija Jugoslavije, Beograd, Nolit.
- Povelja UN, Glava VII, clan 51., https://ius.bg.ac.rs/wp-content/uploads/2020/10/povelja_un.pdf; 14.09.2023.
- Prorokovic, D., (2017), Regionalna bezbednost i teorija realizma: Studija slucaja Arktik, Doktorska disertacija, Fakultet bezbednosti, Beograd.
- Prorokovic, D., (2018), Era multipolarnosti, SluZbeni glasnik, Beograd.Путин, В. (2007). Говор на Конференцији у Минхену 2007. године. Преузето са <https://www.youtube.com/watch?v=hQ58Yv6kP44>, 18.02.2023.
- Стратегия национальной безопасности Российской Федерации до 2020 года, (2009), <https://rg.ru/2009/05/19/strategia-dok.html>., 10.09.2023.
- СТРАТЕГИЯ национальной безопасности Российской Федерации, (2021), <http://static.kremlin.ru/media/events/files/ru/QZw6hSk5z9gWq0plD1ZzmR5cER0g5tZC.pdf> , (09.09.2023).
- Tesanovic, B., (2018), Strukturlni realizam u savremenim medjunarodnim odnosima, Master rad, Fakultet za poslovne studije i pravo, Beograd.

The Alliance`s Strategic Concept, (1999),
https://www.nato.int/cps/en/natohq/official_texts_27433.htm.

Trapara, V., (2020), Ratovi Rsuije 1999-2019, IMPP, Beograd.

Vukadinovic, R., (2001), Medjunarodni politicki odnosi. Zagreb: Agencija za komercijalnu delatnost.

Wohlforth, W. C., (1999), „The Stability of a Unipolar World“, International Security, Vol. 24 Issue 1, Summer 1999.

<https://hcz-zu.hr/evolocija-ruske-strategije-prema-ukrajini/>, 10.09.2023.

<https://vk-spy.ru/bs/animals/vosstaniya-v-stranah-varshavskogo-dogovora-varshavskii-dogovor/>

<https://www.koreni.rs/ratovi-u-sfrj-pocetak-pohoda-na-rusiju/>, 10.09.2023

https://www.vostok.rs/index.php?option=btg_novosti&catnovosti=2&idnovost=139188&RT:-Sporazumi-iz-Minska-dali-Ukrajini-vreme-da-postane-jaca---Merkelova

<https://www.sektorbezbednosti.com/osvrt-na-nove-ruske-predloge-ugovora-o-bezbednosnim-garancijama-sa-sad-i-merama-za-jacanje-bezbednosti-sa-nato-od-17-decembra-2021-godine/>,

mondo.rs/Info/Svet/a1695254/Koji-deo-ukrajinske-teritorije-je-prisvojila-Rusija.html,
12.09.2023

<https://www.slobodnaevropa.org/a/samit-briks-saradnja-johanesburg/32565107.html>.

CHALLENGES OF CRITICAL INFRASTRUCTURE PROTECTION IN CONTEMPORARY SECURITY ENVIRONMENT

Dragisa Jurisic^{1a}

¹ Security Research Center, Street Sinise Mijatovica 9, Banja Luka, Republic of Srpska,
Bosnia and Herzegovina, bicbl@yahoo.com

Received: 28th August 2023

Accepted: 4th September 2023

Original scientific paper

Abstract: *Infrastructures are all around and the life of people in contemporary times depends on them. People are using that infrastructure to make their lives easier and more acceptable. In order to have a nice life people are trying to protect some of that infrastructure. The same situation is with the states. Protection of critical entities or infrastructure is one of the state's tasks when it comes to the basic needs of the population, but these infrastructures usually, in the contemporary world, cross the border, and then there are more subjects responsible for protection. Moreover, some infrastructures are so important and they are in focus for the all world. That kind of infrastructure should be also in some way protected because it has benefits for most of the population in the world. However, the big geopolitical players are calculating depending on their interests whether they would protect that infrastructure or not. This paper shows that world critical infrastructure depends on the interest of big geopolitical players and individual states are not able to do anything to prevent destruction or failure on purpose of that infrastructure.*

Keywords: *infrastructure, geopolitics, protection, security*

(introductory lecture of the forum - work by invitation)

1. INTRODUCTION

Challenges, risks, and threats in the contemporary world are taking on more and more subtle substantive forms, which in a short period of time can threaten vital international subjects or their parts and thus have significant impacts on the development of our civilization.

Natural disasters, the threat of nuclear weapons, terrorism, and hybrid wars remain permanent a threat, and their consequences could have different manifestations. In the coming period, more sophisticated threats such as man-made epidemics/pandemics, attacks with biological and chemical weapons, attacks from virtual space, and hybrid influence will be focused more and more on the vital infrastructures of society and the state, too. Adding to that the indirect and direct endangerment of the natural environment, which causes natural disasters to occur

^a ORCID: 0000-0002-7225-0493

in more frequent periods, creates a picture of an unsafe way of living in the coming period with the impossibility of predicting the ultimate implications.

Critical infrastructure protection is viewed from different positions: technical, defense, economic, national security, etc. The urgency of critical infrastructure protection stems from the fact that these systems are connected and highly vulnerable, and the number of malicious activities directed against processes and activities in society and the state is growing. Criticality assessment is approached from economic, political, and functional aspects. The Economic element indicates the importance of some infrastructure and the entire Economic system. The political aspects take into account the ownership of critical infrastructure, the stability of political conditions or systems in the environments or countries where critical infrastructure is located, and the functional aspect looks at the extent to which the absence of service of a network or infrastructure affects the functioning of the economy, service activities, healthcare, education, and communal services to the preservation of public order and peace and the usual way of life (Maksimovic, 2013).

This paper aims to discuss the topic of critical infrastructure relations on a global scale. It will cover the relationships between major geopolitical players such as Russia, USA, China, India, Great Britain, France, Japan, as well as companies like Facebook, Twitter, Shell, Huawei, and more. The paper will begin by presenting the current security environment, followed by the basics of critical infrastructure protection. It will then provide brief comments on the methodology and focus on specific infrastructures that can have a significant impact on the world if they fail or are destroyed. The paper will also discuss how this impact is manifested or can be manifested globally.

2. CONTEMPORARY SECURITY ENVIRONMENT

Various reports, including EMDAT (2023), highlight the increasing prevalence of natural, technogenic, and anthropogenic hazards in our daily lives. While these threats have existed for centuries, their impact was less significant. There are more than 8th billion people on the planet, billions of factories, cars, trains, planes, buildings, and they depend on electricity, chips, computers, GPS, oil, gas and etc. Most of those entities are very important in order to sustain everyday life. So, they are supposed to be protected in order to sustain our daily routines.

Natural hazards have always existed, and they are not a new phenomenon for humans. However, the way these hazards have impacted people over the last century has completely changed the relationship between humans and nature. Humans have been exploiting natural resources without considering the possibility of replenishing them for future generations. As a result, nature is fighting back and destroying important infrastructure that is vital for human survival and well-being. This is not a conspiracy theory, but rather a consequence of the destructive actions taken by humans towards the environment.

Moreover, there are many technological complexes that support human life on earth or they make it better. Some of those complexes are very dangerous such as nuclear power plants. Any technical failure caused by technological processes, human intervention, or natural hazards can produce huge damage to the population and nature for many years. A similar situation is with the chemical industry which is very dangerous for the population around those facilities. Those factories were built near to the towns but in the last fifty years towns have gotten closer to them and those factories are now in the suburbs of the towns.

However, man, even though it is not the biggest, it is the most significant producer of real dangers. Man can cause, sometimes directly and sometimes indirectly, some natural or technogenic disasters, but a large part of the dangers can still be attributed to man's activities.

His activities and influence on nature, other people, infrastructure, space, etc., can cause huge changes in those areas and in overall human life on Earth. Wars, exploitation of minerals, and deforestation are the most dangerous activities of humans that can cause its destruction.

All those three different types of hazards in the last hundred years are in expansion. Also, there is no possibility to protect everything that is important at all times, and there is no 100% security. Taking it under consideration it is important to decide what kind of “entity” should be protected and which is not so important. In that way, the “critical entities” or “critical infrastructure” are selected.

3. CRITICAL INFRASTRUCTURE PROTECTION

Many scientific papers in the world and neighboring countries discuss the topic of critical infrastructure. Over the past decade, this issue has become a crucial part of security discussions. It has become apparent that safeguarding everything all the time is not feasible and thus must decide which infrastructure holds the highest priority and the reason behind it. Critical infrastructure protection (CIP) is a complex topic that involves politics, business, technology, and risk. Although everyone recognizes the importance of critical infrastructure, there is still no universally accepted definition or list of what constitutes critical infrastructure. This lack of agreement leads to different approaches to defining critical infrastructure and determining how best to protect it.

Despite all this diversity, the common denominator is the importance of that infrastructure. The first broad definition of CI was: "Critical infrastructure consists of those facilities, networks, services and physical and information technology assets that, if interrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning government in member states. Critical infrastructure spans many sectors of the economy, including banking and finance, transportation and distribution, energy, utilities, healthcare, food supply and communications, as well as key government services" (COM (2004) 702).

In particular, the new definition of critical infrastructure given in Directive 2022/5557/EC should be highlighted. According to that document, "critical infrastructure" means an asset, facility, equipment, network, or system or part of an asset, facility, equipment, network, or systems needed to provide the key services. It should be noted that the key term in this document is "critical entity" and the entire document is oriented towards that term, which means that "critical entity" is a public or private entity that the member state has determined belongs to one of the categories given in the document and those categories are divided in there are 11 sectors, ten subsectors, with 52 categories of subjects. This new document on the resilience of critical entities in the EU was prepared based on a study conducted by the European Commission in 2019, study related to the implementation of the previous directive on the identification and marking of European critical infrastructure and the assessment of the need to improve its protection (Directive 2008/114/EC). Directive 2022/5557/EC does not mention European critical infrastructure but critical entities of particular European importance (providing the key services to six or more EU member states).

With these divisions, certain differences were made between key infrastructure, which the EC now calls critical entities, and critical infrastructure, which represents specific elements, thus making a clear distinction and resolving confusion between these two terms, thus clarifying the difference and defining more clearly what is protected. The characteristics of critical infrastructure facilities are:

- Long-term construction - from design to start of work;
- The specificity of the assessment of the endangerment of the object of critical infrastructure;
- Most often, in terms of infrastructure, they are complex constructions (chemical laboratories with auxiliary facilities, school buildings with playgrounds, energy infrastructure facilities - with piers, auxiliary buildings, helipads, etc.);
- Provision of the same is specific;
- Use of specific equipment when performing work and protection activities;
- The destruction or even partial damage of just one object can cause incalculable losses in human and material resources, but also cause the collapse of energy systems, pollute the human environment, or destabilize the banking or financial sector of a country for a long period of time.

For the provision of individual objects of critical infrastructure, an immediate (special) assessment is also carried out, which in principle should contain:

- The state of international relations in the global and regional field (decisions of the main geopolitical actors, decisions and implementation of the activities of organizations and associations in the field of security and defense, etc.);
- Challenges, risks, and threats with indirect and direct impact on the object (situation on the territory, possible types of natural and technical-technological threats, situation in the immediate environment, etc.);
- State of transport, and connections in the environment;
- Cooperation with civil institutions in the environment;
- Required number of personnel and material and technical means and
- The type, strength, and tasks of the personnel guarding the facility.

The protection of each object of critical infrastructure is specific for itself or has specifics that make it different from the others. The constituents of critical infrastructure protection can be divided into three segments: security management that plans, organizes, and implements tasks in the field of critical infrastructure protection; physical security and technical security.

Looking at the characteristics of critical infrastructure from a security point of view is not just a simple sum of factors for which an assessment is made. According to their purpose, such facilities are highly dependent on their way of organizing protection and directly and indirectly dependent on critical infrastructure protection systems in the country.

It should be borne in mind that critical infrastructure will be, in the future, a priority issue for consideration by the government, social, and private sectors. International cooperation and intra-state apparatuses in the modern world provide guidelines, strategies, doctrines, assessments, and other legislative acts that direct development and technical-technological progress, while due to capitalism and the era of globalization, private companies (with or without a share of state capital) specialized in certain disciplines take over jobs.

The destruction of the critical infrastructure elements or destruction in its entirety can cause long-term consequences for the socio-economic life in the area, implying pollution of the human environment, for a long period (no agriculture, investments, transportation, or other activities in that area).

Paying attention to preventive measures is crucial. These measures aim to minimize the likelihood and impact of accidents, and they are: measures foreseen by the selection of technical and technological solutions that ensure the safe transport of hazardous materials within the company; measures that ensure high-quality and timely maintenance of the technical and technological level of the facility - plant, level of knowledge, level of work, and technological discipline; measures intended for the maintenance of communication roads and passages in buildings, plants, and plants and measures provided for in the security system: supervision, management of security and protection systems, detection and identification of hazards (Micovic, 2016).

The main prerequisite for preserving infrastructure as an international entity is to organize its protection. Experience shows that three models of protection can be determined: centralized, decentralized, and integral. Which model individual countries will approach depends on several conditions, the most important of which are the state of security in the country, contractual obligations between the state and the private sector, the geographic position of the critical infrastructure facility, the development of information technologies, etc.

4. METODOLOGY

The main hypothesis in this work is: The contemporary security environment in the world is very challenging in the context of critical infrastructure protection taking into consideration that the biggest geopolitical players are interested in protecting critical infrastructures as long as it is not against their interest.

In this paper, the conclusions were driven, through some examples of the world's important structures and the way the geopolitical players are dealing with them and through analysis of the importance of those infrastructures for the world and their influence in case of malfunctions or destruction.

5. DISCUSSION

To understand challenges in critical infrastructure protection, the best way is to show some real examples. Those situations are interesting from the position of great powers and the geopolitical perspective of world security. The way the countries deal with critical/key infrastructure/entities and the influence of destruction is important but most of the world's critical infrastructures do not depend on them. That kind of infrastructure is in the hands of just 1% of the wealthy Western population. Every day people rely on essential infrastructure like communication, food, and water. However, they lack the ability to safeguard that and to persuade leaders to maintain her safety.

One of the freshest examples is the destruction of the North Stream. In the context of this work, it is not important who did it, it is something else. The North Stream was and is a key infrastructure for the German economy, and it means the European Union economy. Also, it is a key infrastructure for Russia taking into consideration the capacity of the stream and the costs to build it. It became a key infrastructure for two continents. In the end that structure was destroyed. It caused big economic losses for Germany/EU and Russia. Moreover, this structure was destroyed on purpose. One of the conclusions from this example can be that there is no 100% security and there is no structure that cannot be destroyed, on purpose or not. One of the triggers to destroy some infrastructure on purpose can be the geopolitical and economic interest of some states but more and more for big corporations and even individuals who see an opportunity to earn money if that infrastructure is destroyed or damaged. They do not care for ordinary populations and the needs of ordinary people. It is egoism which was not seen up to now, through all history of mankind.

Submarine cables play a critical role in global interconnected networks, carrying about 99 percent of international communications traffic (Brake, 2019). According to “TeleGeography”, in early 2023, there were 552 active and planned submarine cables which are nearly 1.4 million kilometers long (Submarine, 2023). There is a huge amount of information that are going through those cables. Destruction of some of them will have an impact on the world. There are about 200 failures each year and the vast majorities are caused by humans (Griffiths, 2019). However, those are short failures and not made on purpose in most of the cases. Also, natural disasters can cause failure of that infrastructure, too. That key infrastructure exists and works as long as it is important for all to exchange information, earn money, and communicate with each other. Destruction of those cables would cause losses in money and no one is prepared to destroy some of them, yet. Also, there is no full security and it is not possible to protect that entire infrastructure for all time.

Very important world infrastructures are some channels such as Suez Channel and Panama Channel. The last incident with the mega-ship Ever Given, which got stuck in the canal in March 2021, showed all the importance of the channel for the world economy. The same situation is with the Panama Channel which has also a similar role. Moreover, this incident showed that jamming the Suez Channel was very simple to do. That key world infrastructure showed that is very vulnerable. However, the geopolitical players have interests in the Suez Channel depending on their global position and economic benefits. At the moment when some of the world powers decide that the destroyed or jammed Suez Channel could be used for their interests they would easily block it, even destroy it.

In accordance with European Directive 2022/5557 on the resilience of critical entities the space is one of the sectors of critical entities. In that context categories of entities are operators of ground-based infrastructure, owned, managed, and operated by Member States or by private parties, that supports the provision of space-based services, excluding providers of public electronic communications networks. One of those space-based services is communication. Satellite communication services are used every day for telecommunications, TV and radio broadcasting, high-speed Wi-Fi and mobile broadband, navigation and GPS (Global Positioning System) etc. From this point is very important to notice that space and infrastructure over the Earth are crucial for the life of people in these contemporary times. The existence of just one Global Positioning System, which could be vulnerable, and easily blocked or interrupted, pushed other cosmic powers to make and develop their systems similar to GPS (Russian Глобальная навигационная спутниковая система – GLONASS and China The BeiDou - Navigation Satellite System), or to launch their satellites to be independent. In that direction are heading also India, The European Union, and Japan. This kind of communication is very fast but also very sensitive. Today, there are many weapon systems that can intercept signals from satellites, make some interruptions, or even destroy satellites. However, satellites are useful to everyone and all powers are using them. On another hand, satellites can be destroyed very easily and it can cause a world crisis.

Those are just four examples related to infrastructure that can be important for most of the world even if it looks local. That infrastructure depends on the will of geopolitical power would it be destroyed or not and in what percentage, It is a big danger for the world and ordinary people. In that kind of scenario, it is possible to point the finger at some countries, but there will be no consequences for them. It means that 99% of the world's population is at the mercy of global players and the global elite. On them is the decision would we have the internet, access to a bank account, information, what should we watch on TV, what kind of food and from which part of the world would be delivered, how big prices would the population pay for basic needs, etc.

6. CONCLUSION

The importance of infrastructure is directly related to the number of people who could be affected if it were destroyed or stopped from working due to various reasons, such as human actions, technology issues, or natural disasters. While there are numerous sectors and subsectors that can be significant, critical infrastructure should provide essential services such as transportation, energy, finance, healthcare, water, food, communication, and administration. To provide these services, countries use different types of infrastructure and rely, most of the time, on critical infrastructure for global services such as transportation, internet, communication, energy, etc.

However, most of the countries have limited control over this infrastructure. Mostly major geopolitical players ultimately decide whether it will be in functions or accessible, based on their own interests. This means that a single individual or one country can determine whether people worldwide can access certain resources and infrastructures or not.

REFERENCES

Brake D. (2019). Submarine Cables: Critical Infrastructure for Global Communications. Available from: <https://itif.org/publications/2019/04/19/submarine-cables-critical-infrastructure-global-communications/> Accessed: 23.08.2023

COM (2004) 702. Communication on Critical Infrastructure Protection in the fight against terrorism. Final, Brussels. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52004DC0702> Accessed: 28.07.2023.

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. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008L0114> Accessed: 28.07.2023.

Council Directive 2022/5557/EC 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. Available from: <https://eur-lex.europa.eu/eli/dir/2022/2557/oj> Accessed: 28.07.2023.

EMDAT. (2023). 2022 Disasters in numbers: Climate in action, Available from https://cred.be/sites/default/files/2022_EMDAT_report.pdf Accessed: 12.05.2023.

Griffiths J. (2019). The global internet is powered by vast undersea cables. But they're vulnerable. Available from: <https://edition.cnn.com/2019/07/25/asia/internet-undersea-cables-intl-hnk/index.html> Accessed: 19.08.2023.

Maksimovic G. (2013). Model upravljanja kriznim situacijama u Republici Srpskoj, Fakultet za bezbjednost i zastitu. Banja Luka.

Micovic M. D. (2016). Bezbednosni aspekti funkcionisanja kritične infrastrukture u vanrednim situacijama – doktorska disertacija. Univerzitet u Beogradu. Fakultet bezbednosti. Beograd.

Submarine Cable Frequently Asked Questions. Available from: <https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions> Accessed: 20.08.2023.

MASS SURVEILLANCE AND PRIVATE COMPANIES

Sinisa Domazet^{1a}

¹ Educons University, Faculty of Security Studies, Vojvode Putnika 87, Sremska Kamenica,
Republic of Serbia, sdomazetns@gmail.com

Received: 26th June 2023

Accepted: 4th August 2023

Review paper

Abstract: *The rapid development of information and communication technologies, in addition to a large number of positive effects, also brings with it certain dilemmas, one of which is the biggest misuse of modern technologies for the purpose of mass surveillance. Practice has confirmed the existence of a large number of examples of mass surveillance around the world. In the paper, attention is paid to mass surveillance by private companies. It was established that private companies participate to a large extent in mass surveillance, either on their own or if they are left to do so by a special decision of public authorities. Some examples of such activities are analyzed in the paper. The normative method was used in the paper, as well as the legal-logical methods of induction and deduction.*

Keywords: *law, security, internet, mass surveillance, private companies*

(introductory lecture of the forum - work by invitation)

1. INTRODUCTION

The extremely fast development of information and communication technologies, and especially artificial intelligence, has brought numerous challenges, and not only positive effects. As one of the main challenges in the modern world, various technologies for mass surveillance appeared, which very quickly entered every pore of people's lives. It can be said that these technologies have caused a double effect. On the one hand, the supporters of these technologies as an argument in favor of their use point out that in this way it is possible to improve the safety of citizens, reduce the number of criminal acts, and in some places these technologies are also used for the purpose of rewarding citizens for positive forms of behavior in society (such as the case with the social credit system in China). On the other hand, there are also numerous negative features of these technologies.

For example, Privacy International states that mass surveillance “include the direct mass interception of communications, access to the bulk communications stored by telecoms operators and others, mass hacking, indiscriminate use of facial recognition technology, indiscriminate surveillance of protests using mobile phone trackers, and more” (Anon, n.d.).

^a ORCID: 0000-0002-5964-2249

Technologies for mass surveillance are very often the reason for mutual accusations between states. In this regard, the criticisms of Western countries directed at China, due to the social credit system based on mass surveillance technologies, which in this way violate the right to privacy and human rights in general, stand out. As Domazet, Lubura, Susak-Lozanovksa and Ilik said “it is not without reason that the mentioned system, which is essentially based on evaluating and ranking the behavior of officials, businesspeople, and ordinary citizens (with rewards and penalties) has become the subject of wide discussions, not only in the scientific and professional circles in China but also around the globe, primarily in the Western world” (Domazet et al., 2021).

Practice shows that mass surveillance is not always and exclusively carried out by states, but that many private companies around the world are increasingly involved in this activity. In the paper, attention is paid to mass surveillance by private companies. It was established that private companies participate to a large extent in mass surveillance, either on their own or if they are left to do so by a special decision of public authorities. The paper will analyze the activity of private companies in terms of mass surveillance, and then some characteristic examples of such behavior will be listed.

2. ACTIVITIES OF PRIVATE COMPANIES IN PERFORMING MASS SURVEILLANCE

The private sector is becoming more and more present in the field of development and use of mass surveillance tools, as evidenced by numerous publicly available data. Thus, there are data according to which “the mass surveillance industry is a multibillion-dollar industry that has undergone phenomenal growth since 2001” (Anon, 2013). The Wall Street Journal reports that “Intelligence agencies in the U.S. and abroad have long conducted their own surveillance. But in recent years, a retail market for surveillance tools has sprung up from “nearly zero” in 2001 to about \$5 billion a year, said Jerry Lucas, president of TeleStrategies Inc.” (Valentino-DeVries et al., 2011). According to Carnegie, “between 2011 and 2023, at least seventy-four governments contracted with commercial firms to obtain spyware or digital forensics technology” (Feldstein & Kot, 2023).

This report also states that “Israel is the leading exporter of spyware and digital forensics tools documented in the global inventory: fifty-six out of seventy-four governments have procured commercial spyware and digital forensics technologies from firms that are either based in or connected to Israel, such as NSO Group, Cellebrite, Cytrox, and Candiru” (Feldstein & Kot, 2023).

According to some reports, such as “the Report "Video Surveillance Market by Offering (Hardware (Camera, Storage Device, Monitor), Software (Video Analytics, VMS), Service (VSaaS)), System (IP, Analog, Hybrid), Vertical and Geography (North America, Europe, APAC, RoW) - Global Forecast to 2027" “The video surveillance market is projected to grow from USD 48.7 billion in 2022 to USD 76.4 billion by 2027; it is expected to grow at a CAGR of 9.4% during the forecast period” (Anon, 2022).

According to the same report, “Major vendors in the video surveillance market include Hikvision (China), Dahua Technology (China), Axis Communications (Sweden), Bosch Security and Safety Systems (Germany), Hanwha Techwin (South Korea), Avigilon (Canada), Teledyne FLIR (US), Honeywell International; (US), Panasonic i-PRO Sensing Solutions (Japan), Pelco (US), Uniview (China), Agent Video Intelligence (US), CP PLUS (India), Genetec (Canada), Huawei Technologies (China), NEC (Japan), NICE Systems (Israel), Qognify (US), Tiandy Technologies (China), VIVOTEK (Taiwan), MOBOTIX (Germany),

Morphean (Switzerland), Verkada (US), Camcloud (Canada), and Ivideon (US)” (Anon, 2022).

Overall, in the last decade, private companies have taken the lead in the field of mass surveillance technologies. This should not be surprising, taking into account the economic profitability of these technologies, the growing demand around the world, and the fact that the existing legal regulations around the world have greatly limited the room for maneuver of states in exercising surveillance over their citizens. The affair surrounding Edward Snowden showed all the dimensions of indiscriminate mass surveillance of American citizens, and beyond. At the same time, this case has fully opened discussions around the world regarding the preservation of the right to privacy and the mechanisms of its protection.

In terms of legal regulation at the international level, the right to privacy has been the subject of attention of the UN Human Rights Council, as well as the UN General Assembly, whereby it was pointed out that “the same rights that people have offline must also be protected online, including the right to privacy” (United Nations General Assembly, 2015). According to Domazet and Dinic, „privacy is also recognized as a human right in the UN Universal Declaration of Human Rights (Art. 12), as well as in the 1966 International Covenant on Civil and Political Rights“ (Domazet & Dinic, 2022).

In Article 8. of the Convention for the Protection of Human Rights and Fundamental Freedoms, one can also observe the important attitude that “everyone has the right to respect for his private and family life, his home and his correspondence”. It is important to note that this Convention foresees the possibility of suspending the right to privacy, but only “when prescribed by law and necessary in a democratic society in the interests of national security, public security or economic well-being, to prevent disorder or crime, to protect health or morals, or to protect the rights and freedoms of others“.

In addition to this convention, the right to privacy is also important in the Council of Europe Convention for the Protection of Individuals with regard to the Processing of Personal Data (Convention 108+), 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), as well as the African Union Convention on Cyber Security and Data Protection.

When it comes to national regulations governing the right to privacy, most states have their own legislation in this area, where the right to privacy is guaranteed by the constitution in some places, and in some by criminal legislation. Also, in many countries there is special legislation related to the protection of personal data (including Serbia), but there are still countries "where the right to privacy is not recognized as an autonomous right (for example, in the United Kingdom and China)" (Domazet & Dinic, 2022).

Whatever the regulations governing the protection of personal data, i.e. the right to privacy, the fact is that the practice of mass surveillance of citizens in itself causes numerous controversies. On the one hand, there are supporters of the practice of mass surveillance of citizens, who justify it by the need to protect national security from all threats, including terrorist attacks. To this end, it is considered a lesser evil to violate the applicable regulations and some rights of citizens (including the Right to privacy), compared to the danger that is avoided in this way. A typical example is the famous Patriot Act in the USA, passed after the events of September 11, 2001, which provided for surveillance and the possibility of eavesdropping on citizens by security agencies (especially the FBI and NSA), without the prior approval of the judicial authorities. At the same time, this applied to all citizens, not only those

who represent a real security threat to the US, thus legalizing the indiscriminate surveillance of citizens. Practically, the legal regulation that required a court order to be obtained in order to collect sensitive data about citizens was called into question. This was particularly contributed by the rapid development of information and communication technologies and the development of new surveillance technologies, which only made the work of the services easier and made their activities, especially abuses, even less visible than before. It can be argued without exaggeration that services or other bodies that carry out surveillance could practically collect citizens' data without fear of legal consequences and sanctions.

On the opposite side are bitter opponents of the practice of mass surveillance, who believe that mass surveillance must not be allowed under any circumstances, given that it has been shown that in this way the guaranteed human rights of citizens are violated, but also the foundations of modern democratic states are violated. The case of Edward Snowden only gave them a "wind at their backs".

When it comes to practical examples of the actions of private companies in mass surveillance, the famous case of the Pegasus spyware, developed by the Israeli NSO group, should be mentioned. The mentioned software caused a real scandal around the world. It turns out that several member states of the European Union have acquired this software for tracking citizens' mobile phones, under the pretext of preserving national security and fighting terrorism.

According to the media, this is "an advanced type of spyware, that is, a tool used for deep infiltration, primarily in mobile devices, whether they run on Android or EOS Apple's operating system. The possibilities of 'Pegasus' are truly enormous [...] you can access the most diverse content in the phone, practically everything from messages, video content, photos taken, contacts, and the like" (Anon, 2022).

It was the same with the Predator software, which turned out to be even more dangerous than Pegasus. According to open sources, "Predator and its Alien loader have been around since 2019 and are part of a suite of mobile spyware sold by Intellexa." The software, which is designed to spy on and extract data from devices it has entered, is available for Google Android and Apple iOS... This includes recording audio from phone calls and VoIP apps, stealing data from Signal, WhatsApp and Telegram, and even hiding applications or preventing them from starting after the device is restarted" (Anon, 2023).

The above examples clearly show that mass surveillance technologies are increasingly sophisticated and dangerous, and countries around the world are increasingly turning to private companies to ensure the procurement of the latest technological solutions.

3. CONCLUSION

On the basis of what has been said, it can be concluded that the development of modern technologies carries with it a great danger of abuses of various kinds, where one of the most dangerous forms is certainly the practice of mass, indiscriminate surveillance. The affair surrounding Edward Snowden showed all the extent of the misuse of modern technologies for the purpose of mass surveillance. The available data show the existence of a large number of different examples of mass surveillance around the world, with the state and its organs in the foreground. If the practice of the European Court of Human Rights is analyzed, it can be seen that international institutions understand the concept of privacy very broadly, which is an expression of special concern for the preservation of this right.

In this regard, a large number of court decisions that have been made in recent years are very significant, because based on them specific principles have been set when assessing the legality of limiting the right to privacy. This, first of all, refers to the conditions under which state

security authorities can undertake acts of mass surveillance of citizens. Second, acts of mass surveillance must be carried out extremely selectively and proportionally, which implies that the guaranteed human rights of citizens are violated to the least extent possible. Therefore, if it is shown that the goal of surveillance could be achieved by less restrictive methods, in terms of limiting human rights, then the activity of state authorities will not be legal. Finally, a particularly difficult problem is and will be the control of mass surveillance activities (primarily intelligence services) and the protection of the right to privacy. There are numerous discussions on this issue in the world, and independent supervisory bodies have been formed in many countries in order to protect the right to privacy.

In fact, surveillance in itself should not be a problem if it is carried out in accordance with the regulations and based on the approval of the competent authorities. The research showed that it is not only the states that carry out direct mass surveillance with the help of technologies that they have developed themselves, but it is increasingly done through other entities that are not under direct or indirect state influence.

Private companies have proven to be very inventive in the mass surveillance technology market, and revenues from this activity are growing year after year. Also, there is a noticeable growth in the number of these companies around the world, which shows how lucrative mass surveillance has become. Research has shown that private companies participate to a large extent in mass surveillance, either on their own or if they are left to do so by a special decision of public authorities. Therefore, private companies represent a convenient "screen" for activities that the state would not want to be publicly disclosed, given that all state activities (especially those in the field of security) are under the watchful eye of the public.

The presented examples show all the dangers of modern technologies, developed by private companies. Unfortunately, these are only examples that have reached the public. A major problem is the insufficient amount of data regarding the relationship between states and private companies regarding the development of mass surveillance technologies. This cooperation is often shrouded in secrecy, which is regularly justified by the need to preserve national security, while the information about it is marked with the appropriate level of secrecy.

Due to all of the above, the adoption of new or improvement of existing legal regulations, which will protect the right to privacy and other guaranteed rights of citizens in a more efficient way, is of key importance in the future. Practice shows that it is very difficult, due to conflicting interests between states, great resistance to civilian control of intelligence services, insufficiently developed mechanisms for controlling the work of private companies in the field of developing technologies for mass surveillance.

REFERENCES

Anon. (2013). Mass surveillance industry, Available from https://en.wikipedia.org/wiki/Mass_surveillance_industry Accessed: 16.06.2023.

Anon. (2022). Markets and Markets, Available from <https://www.marketsandmarkets.com/PressReleases/global-video-surveillance-market.asp> Accessed: 16.06.2023.

Anon. (2022). Zurnal, Available from <https://zurnal.me/sto-sve-mogu-pegaz-i-predator/> Accessed: 16.06.2023.

Anon. (2023). Informacija. Available from <https://www.informacija.rs/Mobilni-telefoni/Predator-je-komercijalni-spijunki-softver-i-mnogo-je-opasniji-nego-sto-se-mislilo.html> Accessed: 20.06.2023.

Anon., (n.d). Mass Surveillance, Available from <https://privacyinternational.org/learn/mass-surveillance> Accessed: 15.06.2023.

Domazet, S. Dinic, S. (2022). International Legal Aspects of Mass Surveillance and Implications on Privacy, *Culture of Polis*, 19(1), pp. 79-97, ISSN (online) 2812-9466

Domazet, S. Lubura, M. Susak-Lozanovska, I. Ilik, N. (2021). Chinese Social Credit System: New Challenges for the Right to Privacy?, *Journal of Liberty and International Affairs*, 7(3), p. 138, ISSN 1857-9760

Feldstein, S. Kot, B. (2023). Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses Available from: <https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229> Accessed: 16.06.2023.

United Nations General Assembly (2015). The right to privacy in the digital age: resolution, s.l.: United Nations.

Valentino-DeVries, J., Angwin, J. & Stecklow, S (2011). Document Trove Exposes Surveillance Methods, Available from <https://www.wsj.com/articles/SB10001424052970203611404577044192607407780> Accessed: 16.06.2023.

REVIEW OF THE RISKS OF AUTONOMOUS WEAPONS

Katarina Jankovic^{1a}, Nenad Komazec^{2b}, Dražan Erkić³

¹ General Staff of the Serbian Armed Forces, Directorate for Development and Equipping J-5, Technical Test Center, Center for Testing Weapons and Military Equipment, Nikinci, Republic of Serbia, jankovickatarina95@gmail.com

² University of Defense, Military Academy, Veljka Lukica Kurjaka 33, Belgrade, Republic of Serbia, nenadkomazec@yahoo.com

³ Ministry of the Interior – Zvornik Police Department, Svetog Save nn, Zvornik, Republic of Srpska, Bosnia and Herzegovina, dražan.erkic@hotmail.com

Received: 13th September 2023

Accepted: 18th September 2023

Review paper

Abstract: *Weapon autonomy is an imperative for the development of the arms industry. The introduction of autonomous weapons into military conflicts is one of the most current topics in modern warfare. This type of weapon represents a significant advance in the development of technology, but at the same time it also represents a serious risk for the security and stability of states, as well as the global community. This paper analyzes the risks of autonomous weapons. Through problem analysis, this work contributes to understanding the risk of autonomous weapons and finding effective solutions to manage this risk.*

Keywords: *risk, ethics, law, autonomous weapons, artificial intelligence*

1. INTRODUCTION

Acknowledging the weaknesses of artificial intelligence does not diminish its advantages. Artificial intelligence is neither good nor bad; it represents a powerful tool. The key question that arises is how humans should use this technology.

Delegating a task to a weapon implies accepting the consequences if the weapon makes a mistake. When discussing the use of autonomous weapons, it is essential to carefully consider the risks that arise. Weapons designed to harm the enemy can become a danger to one's own units (users) if they go out of control. The significant difference between semi-autonomous (supervised) and fully autonomous weapons is the degree of harm the system can cause before there is an opportunity for human intervention.

In supervised autonomous weapons, humans play the role of a "natural failsafe" who can intervene if problems arise. Humans can override the rigid rules of the system and make decisions. Removing humans diminishes the system's flexibility. In fully autonomous weapons, there is no human to intervene and stop the system's operation. This issue raises

^a ORCID: 0009-0006-0988-4895

^b ORCID: 0000-0001-9227-118X

ethical questions about the future of military technology and how to use it in a way that best serves humanity's interests.

Considering the risks of autonomous weapons extends beyond technical aspects and encompasses broader implications for society, diplomatic relations, and international law. Autonomous weapons present challenges that require careful thought about ethics, security, and the long-term consequences of their use. It also raises the question of how to protect against the misuse of this technology. By examining these issues, a foundation is laid for analyzing how autonomous weapons will shape the future and ways in which society can work together to minimize risks and protect fundamental human values.

2. AUTONOMOUS WEAPONS

Modern weaponry has undergone significant changes in recent years, and one of the most intriguing evolutions is the development of autonomous weapons. Although the concept of autonomous weapons may seem clear, there is actually a considerable level of confusion and ambiguity surrounding its definition. This ambiguity often accompanies questions about the differences between automatic, automated, and autonomous weapons (Figure 1), further complicating the understanding of this technological revolution.

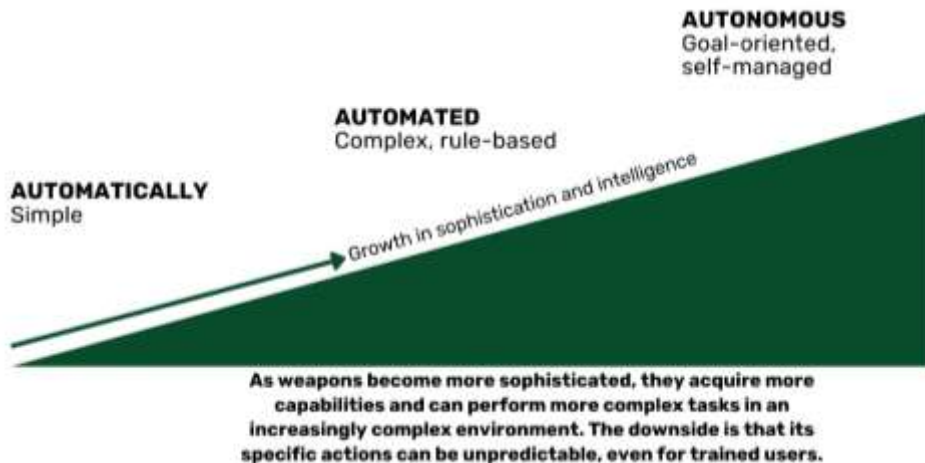


Figure 1. Automatic, automated and autonomous weapons
Source: Created by the authors based on Scharee, 2020

To better understand autonomous weapons, it is necessary to consider a wide range of terms used in relation to modern weaponry. The terminology is often blended, and there seems to be no firmly defined boundary between various categories of weapons. Current terms that emphasize significant characteristics of weapons include: automatic, automated, and autonomous weapons.

Automatic systems are simple and do not exhibit much decision-making. Automatic weapons have evolved gradually, with inventors building upon the work of their predecessors and refining it (e.g., automatic weapons refer to a type of firearm that can continuously fire ammunition as long as the trigger is held down and there is ammunition in the magazine). Automated systems are more complex and can take into account a range of input information and assess multiple variables before taking action (e.g., automated weapons refer to firearms equipped with technology or devices for automating the firing process. This type of weapon can encompass various types of technological enhancements, including electronic targeting and sensors).

Autonomy is the ability of a machine to independently perform a task. There is no internationally agreed-upon definition of autonomous weapons. One definition, used in the working meetings of the International Committee of the Red Cross, states, „Autonomous weapon systems are weapons that can independently select and engage targets, i.e., with autonomy in „critical functions” to acquire, track, select, and attack targets” (International Committee of the Red Cross, 2014).

For ease of use, the terms „autonomous weapon system” and „autonomous weapon” are used interchangeably in this work. Figure 2 illustrates what this entails.

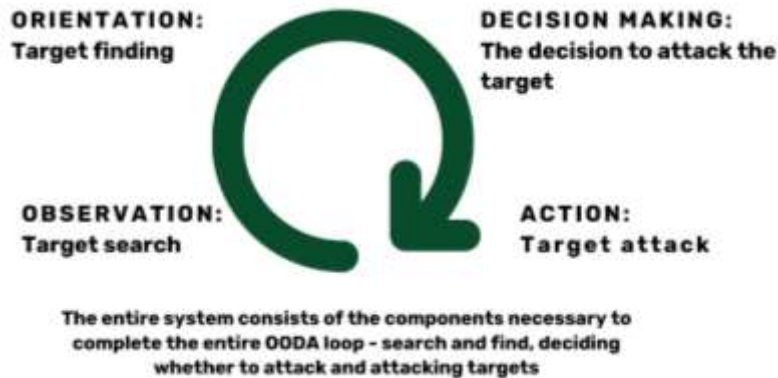


Figure 2. Components of an autonomous weapon
 Source: Created by the authors based on Scharee, 2020

However, depending on the decision-making process for targeting, we differentiate between **supervised autonomous weapons** (human in the loop - Figure 3) and **fully autonomous weapons** (human out of the loop - Figure 4).



Figure 3. Supervised autonomous weapons (human in the loop)
 Source: Scharee, 2020



Figure 4. Fully autonomous weapons (human out of the loop)
Source: Scharee, 2020

If there is a person in the loop deciding which target to engage, it is referred to as supervised autonomous weaponry, as shown in Figure 3 (Scharee, 2020).

In the case of fully autonomous weaponry, as depicted in Figure 4, the entire engagement loop (search, detection, decision, and attack) is automated. Such weaponry can search, make attack decisions, and act independently, with no human intervention possible (Scharee, 2020).

These characteristics create a significant distinction between these two groups of weaponry and determine their purpose.

3. AUTONOMOUS WEAPONS AND ETHICAL CHALLENGES

The use of autonomous weapons may be legal in some situations, but it may not necessarily be morally acceptable. The question of ethical challenges related to autonomous weapons becomes increasingly significant as this technology develops and is applied in military conflicts (Thomas & Mittal 2019). Based on an analysis of relevant literature that examines the ethical challenges of using autonomous weapons, the authors highlight the most significant ones:

Responsibility: One of the primary ethical challenges of autonomous weapons relates to the issue of responsibility. When a machine makes targeting decisions and carries out attacks without human intervention, who is responsible for any unintended consequences? This transfer of responsibility can result in difficulties in establishing blame and ensuring justice in cases of errors or misuse (as the person who activated it may claim not to be responsible for the actions of a system that did not do what the person intended) (Mirkovic, 2007). In contrast, when autonomous weapons correctly execute someone's intent, responsibility is clear: the person who set the autonomous weapon in motion is responsible for it.

Precision and Collateral Damage: Autonomous weapons may be programmed to be precise, but there is a risk of errors occurring in the target identification process. This can lead to "accidental" harm and civilian casualties.

Human Interaction and Decision-Making: With increasing automation in military operations, questions arise about the role of humans in decision-making. Is it morally

acceptable for people to delegate such responsibility to machines, especially in situations involving the use of lethal force? A particular aspect of this element pertains to the use of weapons that are not under the control of organized military or police forces but rather in the hands of terrorists and similar groups.

Lack of Empathy: Autonomous weapons lack the ability to empathize, meaning they cannot understand human emotions and the situations in which people find themselves.

War Crimes and Ethics: The use of autonomous weapons in the context of war crimes poses a unique ethical challenge. How can one identify and sanction those responsible if it is machines that have committed the crimes? This raises questions about justice and moral accountability for such actions.

In light of these ethical challenges, the question arises of how to reconcile technological advancements in the military sector with moral and ethical principles. The international community should continue to address these challenges to ensure that the use of autonomous weapons aligns with the values and principles of humanity.

4. AUTONOMOUS WEAPONS AND LEGAL FRAMEWORK

There have been many attempts in the past to control or ban certain types of weapons, as seen in some examples provided in Table 1. Bans on weapons target different phases of weapon production, preventing access to technology, prohibiting states from developing weapons, restricting production, or regulating use. The legality of autonomous combat systems, like any newly developed weapon, must be assessed based on their design and intended use, as well as their effect on targets (Joncic, 2021).

The laws of war should protect humanity from the worst consequences of war. Modern laws of war were created in the late 19th and early 20th centuries (Scharee, 2020). Today, a series of agreements, such as the Geneva Conventions, constitute the law of armed conflict or international humanitarian law. International humanitarian law (IHL) is the fundamental legal framework for the use of weapons in armed conflicts. IHL applies to all armed conflicts and imposes an obligation to protect civilians, prisoners of war, and the wounded.

IHL has three fundamental principles: the principle of distinction means that armed forces must distinguish between enemy combatants and civilians on the battlefield. IHL recognizes cases where civilians may accidentally suffer harm when targeting enemy combatants, which is known as collateral damage. However, the principle of proportionality states that collateral civilian casualties must not be disproportionate to the military necessity of the attack on a specific target. The principle of avoiding unnecessary suffering prohibits the use of weapons that cause excessive injuries. IHL also includes other rules, such as the protection of combatants who are hors de combat - taken out of action because they have surrendered or are incapacitated (Scharee, 2020).

However, IHL does not explicitly regulate the use of autonomous weapons. IHL principles such as distinction and proportionality apply to the consequences on the battlefield but not to the decision-making process. Historically, soldiers have made the decision to open fire, but nothing in the laws of war prohibits a machine from doing so. Nevertheless, there is a general consensus that IHL can be applied to autonomous weapons, and they should comply with existing norms (Joncic, 1996).

Table 1. Overview of Weapon Bans (Source: (Scharee, 2020; Joncic, 2021; Filipovic, 2023; Mirkovic, 2007)

Red. br.	YEAR	YEAR	REGULATION OR ARGUEMENT	LEGALLY BINDING?	TYPE OF REGULATION	SUCCESS	CONSEQUENCES
1	Serrated bayonets	the first World War	Silent cooperation on the battlefield	Without explicit agreement	Norm against possession	Successful	Unnecessary suffering
2	Submarines	1899. 1921 – 1922.	Hague Convention of 1899 Washington Naval Conference of 1921-1922.	Never ratified	Attempted bans - never ratified	Unsuccessful	Unnecessary suffering
3	Ballistic missile defense	1972.	Ballistic Missile Defense Agreement	Legally binding	Limited deployment	Successful during the Cold War, failed in a multipolar world	Strategic stability
4	Conventional weapons	1996.	Vassenar Arrangement	Legally non-binding	Limited proliferation	Partially successful	Political control
5	Cluster munitions	2008.	Convention on Cluster Munitions	Legally binding	Prohibited development, production, accumulation, and use	Generally successful, with exceptions	Civilian casualties
6	X-ray transparent fragments	1980.	Convention on Certain Conventional Weapons (CCW) Protocol I	Legally binding	Prohibited use	Successful	Unnecessary suffering
7	Incendiary weapons	1980.	CCW Protocol III	Legally binding	Regulated use	Variable success	Civilian casualties
8	Chemical and biological weapons	1985.	Australia Group	Legally non-binding	Prohibited dissemination	Variable success	Civilian casualties, unnecessary suffering
9	Ballistic and cruise missiles	1987. 2002.	Missile Technology Control Regime, Hague Code of Conduct	Legally non-binding	Limited dissemination	There was some success	Strategic stability
10	Intermediate-range missiles	1987.	Intermediate-Range Nuclear Forces Treaty (INF Treaty)	Legally binding	Prohibited possession	Successful but currently threatened in a multipolar world	Strategic stability
11	Nuclear weapons and launcher numbers	1979. 1991. 2002. 2011.	SALT I, SALT II START, SORT New START	Legally binding	Limited quantities	Successful	Limiting the arms race

The United Nations Convention on Certain Conventional Weapons contains some restrictions on the use of weapons that could be applied to autonomous weapons (Joncic, 2021). For example, Protocol III prohibits the use of weapons that may be of little use for targeted destruction or have harmful effects that can spread to the civilian population. However, the application of any form of prohibition is complicated due to the lack of a definition of autonomous weapons.

Despite the unclear regulation in international humanitarian law, the use of autonomous weapons is a reality in armed conflicts. Conflicts in the Gaza Strip have led to serious violations of the rules of international humanitarian law, often due to the use of autonomous and automated weapons. A report by Human Rights Watch documented six incidents in which 29 civilians, including six children, were killed (Joncic, 2021).

In the conflict in Nagorno-Karabakh, Azerbaijan gained a military advantage and victory thanks to the use of such weapons. Armenia did not have a sufficient number of these means and faced limitations, especially in areas where the terrain did not allow the use of conventional weapons.

Managing the risks of autonomous weapons is a challenge for society and requires cooperation between states to establish adequate regulations. Clear legal frameworks are needed to regulate the use of autonomous weapons to prevent unintended consequences and protect human rights. These legal frameworks should cover all aspects of the use of autonomous weapons, including programming, testing, monitoring, and control. International cooperation is also necessary to avoid an arms race in autonomous weapons and to work together to manage the risks posed by this technology. In conclusion, the evolution of the law does not keep pace with the evolution and development of autonomous weapons.

5. AUTONOMOUS WEAPONS IN PRACTICE

In this section, several unwanted incidents related to autonomous weapons are mentioned to better understand the risks associated with this technology that have occurred. Various situations in which autonomous weapons played a role, whether accidents, unwanted events, or serious problems in their use, have been explored. Some of the most well-known examples include (research by the author based on publicly available data):

1. In June 2021, an autonomous howitzer produced by Hanwha Defense suddenly fired a projectile on a cargo ship in the South China Sea while parked on the deck. There were no injuries, but this incident highlights the dangers of unintended activation of autonomous weapons and the need for better control and safety systems.
2. In August 2021, an autonomous mortar produced by Milrem Robotics suddenly activated and fired a mine at a weapons demonstration in Estonia, causing minor damage. This incident highlighted potential dangers of autonomous weapons that are not adequately tested and verified before use.
3. In 2018, an autonomous rocket launcher of Turkish production, KARGU, designed to seek and destroy targets autonomously, fired several rockets at the wrong targets during a military exercise in Turkey.
4. In December 2020, an autonomous combat vehicle produced by General Dynamics Land Systems lost control during testing in the US state of Texas and overturned, killing a worker. This incident highlighted the challenges in developing safe autonomous systems for military use.

5. In March 2020, Turkish Bayraktar TB2 drones, used in the Nagorno-Karabakh conflict, accidentally killed Turkish soldiers. Several such incidents were reported during the conflict.

6. In June 2020, the Iranian anti-aircraft system "Mersad" accidentally shot down a Ukrainian passenger plane after misidentifying it as an enemy aircraft. 176 people were killed.

7. In February 2021, autonomous drones were used in an attack on oil installations in Saudi Arabia. However, the attacks by these drones were unsuccessful, leading to reduced damage that could have been caused but also highlighting the shortcomings in the reliability of this technology.

8. In February 2021, an autonomous rifle produced by TrackingPoint suddenly activated and injured a worker in a Texas warehouse during maintenance. The worker survived, but this incident highlighted potential dangers of autonomously activating weapons.

9. In September 2020, an autonomous border surveillance unmanned system produced by Anduril Industries crashed in Mexican territory, causing a diplomatic incident between the United States and Mexico. This incident highlighted the difficulties in developing reliable autonomous monitoring and security systems.

By reviewing a series of unwanted events related to autonomous weapons from different parts of the world, it is clear that there are significant risks associated with this technology. These events illustrate the potential dangers of unintended activation, target misidentification, accidents during testing, and potential misuse of autonomous weapons.

Such events emphasize the need for stricter safety, reliability standards, and testing rules in the development and use of autonomous weapons. They also point to the importance of adequate training for personnel handling this technology and the need for international regulations that will effectively address ethical and legal dilemmas arising from autonomous weapons.

6. CONCLUSION

Introducing autonomous weapons into armed conflicts brings significant advantages in terms of technological advancement and increasing the efficiency of military operations. However, it also carries serious risks related to safety, ethics, and long-term consequences. The paper has analyzed various aspects of autonomous weapons risks to better understand the implications of their use.

Autonomous weapons can be fully autonomous or semi-autonomous, with or without human intervention. Risks associated with fully autonomous weapons include a lack of human control, accountability for machine errors and decisions, a lack of empathy, and moral dilemmas. Questions about accuracy and collateral damage are also important because autonomous weapons can inadvertently harm civilians or other individuals who are not the intended targets on the opposing side.

Ethical challenges related to autonomous weapons include questions of responsibility, moral dilemmas regarding delegating decisions to machines, and a lack of empathy. It is also emphasized that international humanitarian law, which regulates the use of weapons in armed conflicts, needs to better adapt to autonomous weapons to be applicable.

The legal framework for regulating autonomous weapons is currently unclear, but there are initiatives trying to align existing agreements with new technological challenges. However, more effort is needed to establish clear legal frameworks that will regulate the programming, testing, monitoring, and control of autonomous weapons.

Examples of unwanted events related to autonomous weapons, such as cases of weapons activation during military exercises or unintended attacks on the wrong targets, highlight the need for better safety and control systems.

The future development of autonomous weapons requires strict control. The question of the feasibility of controlling their production and use brings a new dilemma, given that there is now production of highly sophisticated weapons outside of state control. Various cases involve the production of this weapon in controlled state conditions but also abuse by individual states for humanitarian purposes.

REFERENCES

Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects, International Committee of the Red Cross, Expert Meeting, Geneva, Switzerland, March 2014.

Joncic, V. (1996.), „Vojna potreba i medjunarodno pravo”, Vojno delo, 6/96, Beograd

Joncic, V. (2015): Medjunarodno humanitarno pravo, Pravni fakultet, Beograd

Mirkovic, T. (2007): Naoruzavanje i razvoj, Evropski centar za mir i razvoj (ECPD) Univerziteta za mir Ujedinjenih, Beograd

Scharee, P. (2020): Vojska bez vojnika. Laguna, Beograd, 2020. (originalan naslov Army of none: Autonomous Weapons and the Future of War)

Filipovic, A., (2023): Lethal autonomous weapon systems (laws) – towards global regulation or indiscriminate employment?, Politicka revija br. 01/2023, год. (XXXI) XXIII vol. 75

Thomas, R., Mittal, V. (2019): “Potential for Army Integration of Autonomous Systems by Warfighting Function”, Military Review, Army University Press.

Why Should We Ban Autonomous Weapons? To Survive. <https://spectrum.ieee.org/why-should-we-ban-autonomous-weapons>, Accessed: 10.09.2023.

<https://www.britannica.com/biography/Henry-Kissinger>, Accessed: 10.09.2023.

ONE APPROACH TO DETERMINING THE DANGERS TO THE SECURITY-INTELLIGENCE SYSTEM OF THE REPUBLIC OF SERBIA

Nenad Kovacevic^{1a}, Antonio Mak², Zoran Karavidic^{3b}

¹ University of Defence, Military Academy, Veljka Lukica-Kurjaka Street No. 33, 11000
Belgrade, Republic of Serbia, inz.84kula@gmail.com

² University of Defence, Military Academy, Veljka Lukica-Kurjaka Street No. 33, 11000
Belgrade, Republic of Serbia, antoniomak3@gmail.com

³ University of Defence, Military Academy, Veljka Lukica-Kurjaka Street No. 33, 11000
Belgrade, Republic of Serbia, zoran.karavidic@mod.gov.rs

Received: 27th July 2023

Accepted: 10th August 2023

Professional paper

Abstract: *Contemporary challenges, risks and threats to the security of the Republic of Serbia are defined in strategic documents. Challenges, risks and threats are a manifestation of danger. The security-intelligence system of the Republic of Serbia is intended to protect national security from the perpetrators of illegal activities aimed at undermining or destroying the social order established by the Constitution. The aim of the paper is to determine the danger of the security-intelligence system of the Republic of Serbia from the point of view of the risk level. The list of dangers has been made based on the results of the research. Due to the length of the paper, only a brief overview of the methodology and results of the research is given.*

Keywords: *danger, challenges, risks, threats, security*

1. INTRODUCTION

Contemporary times are marked by conflicts that are a real threat to global security, as they produce a large number of civilian casualties and force millions to leave their homes. The modern era brings with it many unpredictable news that testify that the intervals between world crises are getting shorter, the scope and complexity of modern crises are increasing rapidly, leaving little or no time for planning. We are witnessing a very dynamic multidimensional and asymmetric process because globalization takes place unevenly in different dimensions, i.e. It is a complex process that covers equally economic, military, legal, ecological, cultural and social aspects.

In such security conditions, many countries have decided to build their national security on the "wagon" principle – tying their national security to one of the world powers or military-political alliances. The Republic of Serbia is a militarily and political neutral state. Therefore,

^a ORCID: 0000-0002-0840-0063

^b ORCID: 0000-0002-4989-8793

preserving the national security of the Republic of Serbia is a very complex task that has been entrusted to us security-intelligence system of the Republic of Serbia.

The main focus of the paper is the determination of dangers per the security-intelligence system of the Republic of Serbia from the point of view of the probability of their occurrence and the severity of the consequences, that is, through risk assessment. The above is important primarily because it represents a guideline for further dealing with dangers according to priorities. The paper presents the results of the research conducted with the aim of obtaining the answer to the research question: "Defining the dangers of the security-intelligence system of the Republic of Serbia according to the risk level?" The dangers that was used for the purposes of the research are actually the challenges, risks and security threats defined in the National Security Strategy of the Republic of Serbia (hereinafter: The Strategy). The paper consists of three parts, the first part of the paper is dedicated to the security-intelligence system of the Republic of Serbia; the second part of the paper presents the conceptual definition of danger, challenges, risks and security threats, while the research protocol and results are presented in the third part of the paper.

2. SECURITY-INTELLIGENCE SYSTEM OF THE REPUBLIC OF SERBIA

The historical development and shaping of the security system in various periods undoubtedly indicates its dependence on political structures and the state. It is an apparatus of government that has always been under the scrutiny of politics. It can be said that every government is the foundation of a political system that represents an essential component of political processes in society. The security system is a complex, dynamic and specific subsystem in the development of every society (Dragisic, 2020).

The security-intelligence of the Republic of Serbia is intended to protect national security from the perpetrators of illegal activities aimed at undermining or destroying the social order established by the Constitution. For that purpose, multiple intertwined preventive and reactive measures and activities are undertaken. In cooperation with the bodies of the executive and judicial authorities, internal and external carriers who are thus prevented (disabled) from threatening the security of vital state values, that is, national security, are discovered and monitored.

The security-intelligence system is a constituent of the national security system of the Republic of Serbia. The security-intelligence system, according to the Law on the Basics of the Organization of the Security Services of the Republic of Serbia, consists of the following organizational structures: National Security Council, Bureau for the Coordination of Security Services, Security Services and Committee of the National Assembly for Supervision of the Work of Security Services. (Zakon o osnovama uredjenja sluzbi bezbednosti Republike Srbije, 2012) Connections and relationships between system elements are shown in Figure 1, solid lines indicate subordination, and dashed lines indicate information flow.

The *National Security Council* consists of the following members: the President of the Republic, the Prime Minister, the Minister, the Minister of Internal Affairs and Justice, the Chief of the General Staff of the Serbian Armed Forces and the directors of the security services. On the basis of the Law on the Basics of Organization of Security Services, the Council has a clear scope. The method of work is specified by certain internal acts – the Rules of Procedure of the Council (Kovacevic et al., 2018).

The *Bureau for the Coordination of Security Services* (hereinafter: the Bureau) is an operational body that coordinates the work of the security services and executes the conclusions of the Council within its jurisdiction. This implies that the Bureau: determines the method of operational harmonization in individual cases; determines the tasks that are

performed by operationally coordinating the activities of the security services and other state bodies; establishes mixed working groups for operational tasks; analyzes the results of operational alignment and reports to the Council. The bureau consists of the directors of the security services and the secretary of the Council by position, but without decision-making rights. Representatives of the Ministry of Foreign Affairs, the director of the police and heads of police departments, the Republic Public Prosecutor, the director of the Customs Administration and managers of other state bodies, institutions and organizations can participate in the work of the Bureau by invitation (Kovacevic et al., 2018).

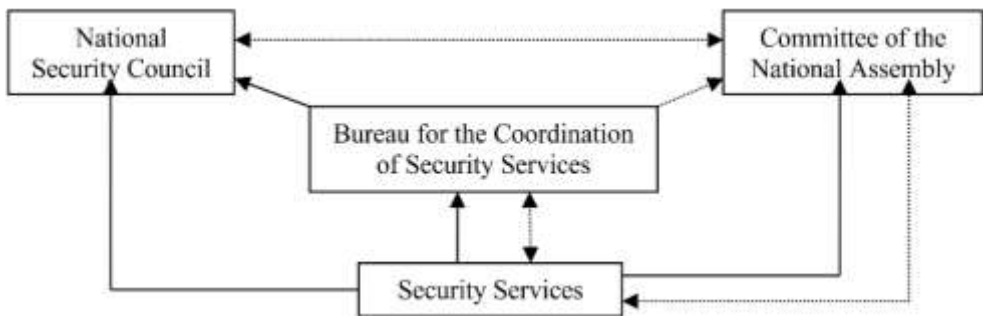


Figure 1. Schematic representation of the security-intelligence of the Republic of Serbia
Source: Author

The *security services of the Republic of Serbia* represent a specialized, relatively independent institution of the state apparatus authorized to collect security data and information about other countries and its institutions, as well as about possible enemies, by legal, public, but also secret ways and means, for the purpose of conducting state policy. The security services have a long tradition, and under the influence of social and political changes in the country, they underwent a certain degree of reorganization. They act on the basis of and within the framework of the Constitution, laws, other regulations and general acts, the national security strategy, the defense strategy and the established security and intelligence policy. All members of the security service must act in accordance with the above, according to the rules of the profession, politically neutral and impartial (Zakon o osnovama uredjenja sluzbi bezbednosti Republike Srbije, 2012).

The *Committee of the National Assembly for Supervision of the Work of Security Services* is the highest legislative body for democratic and civilian control of the security services. The constituents of the security system are the state and its citizens, while the subjects are the following: professional subjects of the security system; political subjects of the security system; and supplementary subjects of the security system (Kovacevic et al., 2018).

The work of the security services in the Republic of Serbia is under the democratic and civilian control of the National Assembly, the President of the Republic, the Government, the National Security Council, as well as other state bodies and the public, i.e. citizens. The supervision of the work of the security services is based on the following principles: political, ideological and interest neutrality of the security services; subordination and responsibility of the security services to the elected authorities of the Republic of Serbia; duties of supervisors to inform the public about their results; obligations of the security services to inform the public about the performance of their tasks in accordance with the law; professional responsibilities and operational independence of members of the security services in the execution of assigned tasks and the responsibilities of managers for the work of the services (Zakon o osnovama uredjenja sluzbi bezbednosti Republike Srbije, 2012).

3. CHALLENGES, RISKS AND THREATS TO THE SECURITY OF THE REPUBLIC OF SERBIA

The basic terms of security grammar are: danger (what threatens), reference object of security (what is threatened) and means and measures of security (the way to protect) (Ejdus, 2012). "Danger is a potentially harmful physical event, phenomenon or human activity that can cause endangerment of human life and health, damage to material and cultural assets and the environment, or social and economic disturbances." (Zakon o smanjenju rizika od katastrofa i upravljanju vanrednim situacijama, 2018). The probability of occurrence and the severity of the consequences of danger to the safety reference object represent a risk, that is, the uncertainty of achieving the goals. This term should not be confused with the term used in the Strategy.

Danger can manifest as a challenge, risk or threat. Although these three types of dangers are often spoken together without making a clear conceptual distinction between them, these terms do not have the same meaning (Ejdus, 2012).

A challenge is a situation that puts someone or something to the test. This situation can have a negative or positive outcome (Ejdus, 2012). It represents the least harmful form of danger in terms of content and consequences, and in terms of time it is the farthest danger from the protected value. It is about the apparent phase of the danger which may or may not be realised and which is incorporated in the possible intention of its bearer (Bajagic, 2007).

Risk is defined as possibility of loss, injury, inconvenience or destruction. Unlike challenges, risk generally has a negative meaning (Ejdus, 2012). Security risk can be viewed as: "a specific form of danger since it is inherent to both the subject of security and the subject of danger. The two-sidedness of a security risk is that both subjects exist in an uncertain security environment and continuously make decisions about their own engagement, and each decision is accompanied by a certain risk." (Mijalkovski & DJordjevic, 2007).

A threat is a conscious intention to cause harm to a person, property or right in order to force the object of the threat to comply with the imposed behaviour. A more concrete phenomenon is the one whose occurrence is the least uncertain, while the harmful effects are the greatest and indisputable (Lazic, 2014).

The Strategy contains the list of the most significant challenges, risks and threats to the security of the Republic of Serbia: armed aggression, separatist aspirations, illegally unilaterally declared independence of the territory administratively included in the Autonomous Province of Kosovo and Metohija, armed rebellion, terrorism, proliferation of weapons of mass destruction, ethnic and religious extremism, intelligence activities, organised crime, drug addiction, mass illegal migrations, problems of economic development, problems of demographic development, epidemics and pandemics of infectious diseases, energy security, the unfinished process of demarcation of the countries of the former SFRY, natural disasters and technical and technological accidents, climate change, and the rise of high-tech crime and threats to information and communication systems (Strategija nacionalne bezbednosti Republike Srbije, 2020). The stated security challenges, risks and threats were used for the purposes of research, as threats to the security-intelligence system of the Republic of Serbia for which a risk assessment is carried out.

It is important to point out here, the Strategy recognises other challenges, risks and security threats, such as: "corruption, misuse of new technologies and scientific achievements, genetic engineering, medicine, meteorology and other scientific fields. They often do not exert an open influence on the security of the Republic of Serbia, so it is difficult to detect them and recognise the patterns of their activity." (Strategija nacionalne bezbednosti Republike Srbije, 2020).

4. REVIEW OF RESEARCH

The research method used in the paper is a combination of several methods, namely the method interview, matrix and the statistical method, even though it was inevitable to implement the methods of expert evaluations, analysis and synthesis, and induction and deduction in the research process. The entire research process is intertwined with these five methods, and the basic question is defining the dangers of the security-intelligence system of the Republic of Serbia according to the risk level. The goal of applying the interview method, matrix method and the statistical method is to determine the dominant views on the subject of the research paper, as well as to summarise the existing information on the subject of the research, while at the same time avoiding discrepancies in the opinions of experts. The research approach applied in the paper includes three phases: (1) research planning, (2) research implementation and (3) analysis of research results. The following stages of the research process are elaborated on in the remainder of the paper.

4.1. Research planning

In order to implement research planning, a research protocol has been defined, and it contains the following elements: research aim; research question; formation of an expert group; defining the research tool – survey questionnaire; data extraction and the synthesis of the extracted data.

The aim of the research has been to perform, at the level of scientific description, an analysis of the opinions received by experts concerning the defining dangers of the of the security-intelligence system of the Republic of Serbia according to the probability of their occurrence and the severity of the consequences. The realisation of the defined research aim is achieved by answering the research question:

RQ: *"Defining the dangers of the security-intelligence system of the Republic of Serbia according to the risk level?"*

The formation of the expert group was carried out through several stages: determination of the size of the expert group, selection and assessment of the competence of experts and definition of agreement of expert evaluations. Due to the extensiveness of the procedure for the formation of the expert group, only a brief overview of the implementation of the previously mentioned phases will be presented here. For the purposes of the research, the following experts were selected: retired and active members of the security agencies, as well as the members of the academic community whose sphere of interest is national security. Since this is the population of unknown size, the size of the expert group was determined according to the previously published model (Kovacevic, 2021). According to the aforesaid model, the minimum size of the expert group is 16. The selection of experts was made using the "snow avalanche" method. By applying this method, a potential group of 34 experts was determined. The assessment of experts' competence was carried out using the Dobrov's method and the Russian method. (Kovacevic, 2021) By applying the aforementioned methods, out of 34 potential experts, 18 people were selected as experts by competence assessment.

The survey questionnaire consisted of two parts, in the first part the experts entered their personal data, which were necessary for evaluating their competence (according to the combined method that includes the Poland method and the Dobrov's method); while in the second part the questions related to the probability of occurrence and severity of the consequences of certain dangers of the security-intelligence of the Republic of Serbia were formulated.

Data extraction was performed on the basis of the answers to the questions from the survey questionnaire, and *the synthesis of the extracted data* was performed using the statistical method, more specifically positional average values, with a previous analysis of the agreement of expert evaluations (opinions).

4.2. Research implementation

After defining the expert group (size and competence) and creating the survey questionnaire, the survey was conducted. The survey was conducted electronically in such a way that the experts received the questionnaire via e-mail and returned it to the researcher. After receiving expert evaluations, their agreement was analysed using the concordance test (W), Concordance test is, the correlation coefficient of the ranks for the expert group, as a measure of the agreement of the experts. The concordance coefficient tests the relationship between the actual and the maximum possible agreement of the experts, and varies within [0,1], where a value of 1 means that all experts gave the same ratings, and a value of 0 means that there is no relationship between the expert ratings. After processing the answers of the experts, the concordance coefficient was calculated $W=0,395$ which, according to the table values, proves that the deviations are minimal in relation to the sample size (Petz, 1997) Since it was established that there is a correlation of expert evaluations, there was no need to conduct interviews with individual experts, that is, there were no drastic deviations of experts' opinions (differences in expert evaluations) within the group. The above represents a quantitative processing of expert evaluations. After receiving the expert evaluations, their analysis was performed using the positional average value - mode, and then a conclusion was drawn, which is a qualitative analysis of the expert evaluations. (Kovacevic et al., 2022)

4.3. Analysis of the research results

After the quantitative, a qualitative analysis of the research results was performed. A matrix method was used for risk assessment, specifically the 5x5 risk matrix (MIL-STD-882B) with five levels of risk. In the survey questionnaire itself, the experts were first offered nineteen dangers taken from the Strategy, then to rate the probability of occurrence of each danger on a scale from 1 to 5, where 1 – Very Unlikely, 2 – Unlikely, 3 – Possible, 4 – Likely and 5 – Very Likely, then to rate the severity of the consequences of each danger on a scale from 1 to 5, where 1 – Negligible, 2 – Minor, 3 – Moderate, 4 – Significant and 5 – Severe. (Kovacevic et al., 2019) Results of expert evaluation are shown in Table 1.

Table 1: Results of expert evaluations

Name of the danger	Probability	Consequences	Risk	Level
Armed aggression	3,94	4,44	17,50	High
Separatist aspirations	3,11	3,61	11,23	Medium
Illegally unilaterally declared independence of the territory administratively included in the Autonomous Province of Kosovo and Metohija	3,11	2,72	8,47	Medium
Armed rebellion	2,72	3,05	8,31	Medium
Terrorism	3,22	3,44	11,09	Medium
Proliferation of weapons of mass destruction	2,55	3,50	8,92	Medium
Ethnic and religious extremism	3,72	3,94	14,67	Medium High
Intelligence activities	3,61	4,50	16,24	High

Name of the danger	Probability	Consequences	Risk	Level
Organised crime	4,06	4,28	17,37	High
Drug addiction	2,39	2,28	5,44	Low Medium
Mass illegal migrations	3,72	4,33	16,11	High
Problems of economic development	4,22	4,28	18,05	High
Problems of demographic development	3,00	3,33	9,99	Medium
Epidemics and pandemics of infectious diseases	4,39	4,44	19,51	High
Energy security	4,50	4,33	19,50	High
The unfinished process of demarcation of the countries of the former SFRY	1,67	2,00	3,34	Low
Natural disasters and technical and technological accidents	3,11	3,33	10,37	Medium
Climate change	2,78	2,72	7,57	Low Medium
The rise of high-tech crime and threats to information and communication systems	3,89	4,22	16,42	High

The values in the "Probability" column were obtained by multiplying the number of experts who agreed with the value of the division of the scale, adding them and dividing by the number 18. The same principle is applied to get the values in column "Consequences". Values in the column "Risk" are obtained by multiplying the values from the columns "Probability" and "Consequences". The level of risk is determined according to the following from 0 to 4,00 Low; from 4,01 to 8,00 Low Medium; from 8,01 do 12,00 Medium; from 12,01 to 16,00 Medium High and from 16,01 to 25,00 High. Risk is considered to be unacceptable, if it is estimated to be Very High and High, and acceptable, if it belongs to the field of secondary (Medium, Low Medium) or Low risk.

5. CONCLUSION

The paper presents the results of research aimed at answering the research question: "*Defining the dangers of the security-intelligence system of the Republic of Serbia according to the risk level?*" The research results are significant in three aspects. Firstly, dangers to the security-intelligence system of the Republic of Serbia were evaluated according to probability of occurrence and severity of consequences for the system. Secondly, the research results provide guidelines for further treatment of dangers, depending on whether they are in the field of acceptable or unacceptable risk. Thirdly, the research results from the point of view of the consequences of certain danger show which parts of the security-intelligence system are particularly threatened.

Based on the research results, it can be concluded that the following threats to the security-intelligence system fall into the field of unacceptable risk: epidemics and pandemics of infectious diseases, energy security, problems of economic development, armed aggression, organised crime, intelligence activities, mass illegal migrations and ethnic and religious extremism. The paper presents one of the approaches to determining the dangers to the security-intelligence system of the Republic of Serbia.

REFERENCES

- Bajagic, M. (2007). Osnovi bezbednosti, Kriminalisticko-policijska akademija, ISBN 86-335-0190-7, Beograd
- Dragisic, Z. (2020). Sistem nacionalne bezbednosti Srbije, Fakultet bezbednosti, ISBN 978-86-80144-40-5, Beograd
- Ejdus, F. (2012). Medjunarodna bezbednost: teorija, sektori i nivoi, JP Sluzbeni glasnik & Beogradski centar za bezbednosnu politiku, ISBN 978-86-519-1236-1, Beograd
- Kovacevic, N. (2021). Model procene rizika upotrebe pontonirskih jedinica u vanrednim situacijama, doktorska disertacija, Vojna akademija, Univerzitet odbrane u Beogradu, Beograd
- Kovacevic, N. Mak A. Kovac, M. (2018). Current problems in functioning of the National Security Council of the Republic of Serbia, International Scientific Conference „Archibald Reiss Days”, ed. Dane Subosic, pp. 283-292, ISBN 978-86-7020-405-8, Belgrade, October 2018, Academy of Criminalistic and Police Studies, Belgrade
- Kovacevic, N. Mak, A. Teodorovic, B. (2022). Challenges, risks and threats to the security of the Republic of Serbia, Proceedings 8th International Scientific Conference Security and crisis management, ed. Nenad Komazec, Branko Babic, pp. 81-87, ISBN 978-86-80692-09-8, Sremska Kamenica, September 2022, Regional Association for Security and Crisis Management, Belgrade
- Kovacevic N. Stojiljkovic, A. Kovac M. (2019). Application of the matrix approach in risk assessment, Operational Research in Engineering Sciences: Theory and Applications, 2 (3), pp. 55-64, ISSN: 2620-1607
- Lazic, R. (2014). Kontrola sluzbi bezbednosti u Srbiji, Kriminalisticko-policijska akademija, ISBN 978-86-519-1868-4, Beograd
- Mijalkovski, M. Djordjevic, I. (2007). Neuhvatljivost nacionalne moci, Sl. glasnik RS, ISBN 978-86-519-0715-2, Beograd
- Petz, B. (1997). Osnovi statisticke metode za nematematicare, 5. izdanje, Naklada Slap, ISBN 953-191-058-8, Zagreb
- Strategija nacionalne bezbednosti Republike Srbije. (2020). Sluzbeni vojni list, broj 2/2020, Beograd
- Zakon o osnovama uredjenja sluzbi bezbednosti Republike Srbije. (2012). Sluzbeni glasnik RS, broj 116/2007 i 72/2012, Beograd
- Zakon o smanjenju rizika od katastrofa i upravljanju vanrednim situacijama. (2018). Sluzbeni glasnik RS, broj 87/2018, Beograd

CRITICAL INFRASTRUCTURE PROTECTION IN SOME BALKAN COUNTRIES IN COMPARISON WITH BOSNIA AND HERZEGOVINA

Zeljko Zoric¹

¹ Sector Security, Street Sinise Mijatovica 9, Banja Luka, Republic of Srpska, Bosnia and Herzegovina, zoriczeljko1@hotmail.com

Received: 10th July 2023

Accepted: 10th August 2023

Professional paper

Abstract: *Frequent social changes, acts of terrorism and war, climate changes, often lead to temporary or permanent damage to critical infrastructure. Precisely because of the consequences, critical infrastructure protection is a frequent topic of discussion in the scientific and professional public. The first step in action when it comes to critical infrastructure protection is the adoption of legal acts what will define critical infrastructure as well as the measures for its protection. In this regard, the countries surrounding Bosnia and Herzegovina have already come a long way, driven by the real internal needs and EU requirements. Entities in Bosnia and Herzegovina, as well as the existing District, have not taken significant steps in the field of critical infrastructure protection. In this paper, the legal solutions for critical infrastructure protection in Bosnia and Herzegovina, Croatia and Serbia are presented using the method of comparison and content analysis.*

Key words: *critical infrastructure, law, protection, comparison*

1. INTRODUCTION

With the establishment of the first social communities, certain values arose that had to be protected, the values whose damage or destruction would question the survival of the entire community, With the civilization development, certain measures also developed, that is, ways of protecting social values, which today we call by a unique name – critical infrastructure.

The beginning of the 21st century marked, among other things, a renewed focus on critical infrastructure protection, especially in the West, as a result of increased concern for the provision of basic needs such as energy and transport. However, instead of the earlier focus on the danger of large-scale armed conflicts, “new” uncertainties are increasingly coming to light, primarily because of the increasing critical infrastructure complexity and interdependence. Therefore, instead of the danger of conventional military conflict, increasingly present cyber threats in the conditions of interconnected and networked infrastructures are being considered. (Milosavljevic & Komazec, 2021).

Critical infrastructure networking and its distribution certainly crosses national borders, and therefore its protection have a different significance. Namely, contemporary threats very often

surpass national borders and therefore affect the multinational response. An obvious example is climate change, which has led to significant change in the form of increasingly frequent heavy rainfall and long-lasting droughts in an unexpectedly short period of time. These changes threaten infrastructure to a great extent in almost all countries and therefore require a unique response. Even though we try very hard to pay attention to these causes, it is also necessary to return to somewhat neglected threat to infrastructure, and those are the ones caused by war operations. The current military conflicts between Russia and Ukraine have brought to surface the threats to all infrastructure segments. According to the available data, which derive from the official reports of the parties involved in this conflict, it is evident that infrastructure destruction is brutal and neither side takes into account the consequences that remain, on civilians and nature. Electric power system facilities, roads food production, etc. are particularly at risk. The new situation represents a serious test for the adopted protocols for critical infrastructure protection from threatening phenomena, regardless of the time, place and manner of their manifestation. Large countries can allow themselves to independently develop a critical infrastructure protection system, even though it may turn out not to be a good solution.

The recent earthquake in Turkey has shown that this territorially large and populous country is not able to respond independently to such an accident that caused significant damage to the infrastructure in all aspects. The European Union, with its infrastructure, certainly represents a serious challenge to protect it from various endangerment forms. The existing system certainly has its advantages and disadvantages when it comes to measure implementation in real situations of endangerment. The recent corona virus epidemic, as well as the current situation in Ukraine, as two diametrically opposite causes, put the existing EU protection measures to a serious test.

Protection measures against the corona virus have shown that they are not very effective, i.e., that EU member states made decisions very quickly that were not in accordance with the EU's unique measures. Almost overnight, the member states re-established a hard border in places where it had been abolished some time ago. The wartime destruction of infrastructure in Ukraine is certainly a serious concern for the EU and will influence the revision of the existing critical infrastructure protection system. Countries that are now members of the EU, but have an intention of becoming one, such as Serbia, adopt laws and measures that follow the recommended standards and develop critical infrastructure protection system that would be isomorphic with the system that exists in the EU. When it comes to Bosnia and Herzegovina with its entities and districts, it is evident that it represents an "isolated island" in Europe without any organized measures to protect critical infrastructure.

2. CRITICAL INFRASTRUCTURE PROTECTION IN THE EUROPEAN UNION

The European Union has recognized the importance of critical infrastructure protection, i.e., the consequences that would occur if it were threatened. The latest threat to critical infrastructure, as a consequence of the corona virus pandemic, put the existing critical infrastructure protection system to a serious test. It has been shown that critical infrastructure is no longer and cannot be the responsibility of one state only, i.e., we are talking about critical infrastructure whose protection is regionally connected. In order for the EU to adopt uniform measures and procedures, it was necessary to adopt a uniform definition of critical infrastructure, which reads: "Critical infrastructure is an asset, system or a part of it, located in the territory of a member country and which is necessary for the maintenance of key social functions, healthcare, safety, security economic or social well-being, and the disruption or destruction of which would have a significant impact on the member country".

European Program for Critical Infrastructure Protection (EPCIP) from December 12, 2006 set a general framework for activities aimed at improving critical infrastructure protection in all EU countries and in all relevant sectors of economic activity.

Four main focus areas of EPCIP were then developed:

1. Procedure for European critical infrastructure identification and designation and assessment of the need to improve their protection is detailed in Council Directive 2008/114/EC;
2. Measures designed to enable the EPCIP implementation, including action plan, the Critical Infrastructure Warning Information Network (CIWIN), the use of CIP (Critical Infrastructure Protection) expert groups at the EU level, the CIP information exchange process and identification and interdependency analysis;
3. Financing CIP-related measures and projects that focus on prevention, preparedness and management of terrorism consequences and other security-related risks for the period 2007-2013;
4. EPCIP external dimension development (Kekic, 2019).

Directive 2008/114/EC is the basis for the next steps in defining criteria for critical infrastructure. Annex III of this Directive lists the procedures, which each member country should implement, through several consequent steps. EU critical infrastructure protection is also based on critical infrastructure protection in the fight against terrorism (COM (2004) 702 final, October 20, 2004); Green Paper on the European Program for Critical Infrastructure Protection (COM (2005) 576 final, November 17, 2005); Communication from the Commission on the European program for critical infrastructure protection (COM (2006) 786 final, December 12, 2006). Working document of the Commission service on a new approach to the European program for critical infrastructure protection – Additional insurance of European critical structures (SWD (2013) 318 final, 28/08/2013).

Strategic agenda for 2019-2024 which was adopted by the European Council in June, requires a comprehensive approach to protect Europe from malicious cyber activities and hybrid threats. The European Commission assessed the 2008 Directive on critical infrastructure protection. The assessment shows the evolution of threats facing Europe. The evaluation also emphasizes that the EU's approach towards critical infrastructure protection must be flexible and risk-based to reflect the threats and vulnerabilities critical infrastructure is likely to face in upcoming decades. The assessment suggests that there are additional sectors that member states consider worthy of additional protective actions at the European level. Based on the evaluation findings, there are reasons to examine the scope of the EU critical infrastructure framework with the aim of including additional sectors (Kekic, 2019). If the corona virus pandemic tested the critical infrastructure protection system in the EU, the conflict in Ukraine certainly influenced the need to raise a serious question about the critical infrastructure protection functionality in the EU. That there have been serious changes in the understanding, definition and protection of critical infrastructure is clear from the "introduction" of the NATO structure and forces in critical infrastructure protection. NATO and the EU launched a work group to strengthen critical infrastructure in response to the "attack" on the Nord Stream gas pipelines and Russia's use of energy as a weapon in early 2023. This work group consists of NATO and EU experts tasked with identifying key threats to critical infrastructure, to assess vulnerabilities and an appropriate response. This is, at the same time, critical infrastructure protection militarization in which there is no place for civilian planning and management, which again questions numerous previously adopted documents at the EU level that do not take into consideration critical infrastructure only. That such a work group is a concept

previously prepared, for something new in the future, can be concluded from the fact that it has not yet been proven who is guilty of sabotage on the Nord Stream.

3. CRITICAL INFRASTRUCTURE PROTECTION IN CROATIA

With the Law on Critical Infrastructure Protection from 2013 and 2022, Croatia took over the EU regulations contained in Council Directive 2008/114/EC from 2008 on European critical infrastructure identification and determination and the assessment of the need to improve their protection. Croatia adopted the Law on Critical Infrastructures (Croatian Parliament, 2013), the Decision on determining the sector from which central state administration bodies identify national critical infrastructures and lists of critical infrastructure sector sequence (Government of the Republic of Croatia, 2013), Rulebook on Methodology for creating critical infrastructure risk analysis operations (DUZS director, 2013). In order to improve and align with international standards, in 2016, a new Rulebook based on the ISO 31000:2009 standard (instructions and guidelines for risk management) was adopted and applied.

Laws and by-laws regulate the critical infrastructure risk management area, with regards to: the exposure of the Republic of Croatia to dangers, both of natural origin and those caused by technical and/or technological processes, which include exposure to terrorist activities, both in real and in cyberspace, that Croatia is particularly sensitive to threats to its critical infrastructures because its resources do not allow it to fully develop alternative/redundant systems, and this sensitivity is increased by the connection and interdependence of numerous sectors both at the national level and with critical infrastructure sectors both at the national level and with critical infrastructure sectors of neighboring and other countries, that this area represents the backbone of national and public security and sustainable development and progress of key interest, both for the population/individuals, as well as for the overall economy, social activities and the country as a whole. In July 2018, the Croatian Parliament adopted the Law on Operator Cybersecurity of Key Services and Digital Service Providers, which transposed Directive 2016/1148 of the European Parliament and the Council of the EU on measures a high common level of network and information system security throughout the Union into Croatian legislation, which regulates the area of critical infrastructure information and communication security. Achieving the highest level of critical infrastructure and population safety and protection is determined by the first strategic goal of the National Security Strategy of the Republic of Croatia (Government of the Republic of Croatia, 2017). The State Administration for Protection and Rescue of the Republic of Croatia has adopted the Rulebook on the methodology for the critical infrastructure risk analysis operations, which “establish the guidelines, criteria and benchmarks for the critical infrastructure operation identification and risk analysis, as well as the holders and their obligations of critical infrastructure business risk analysis which is an integral part of the risk assessment process.” The Rulebook was published in the Official Gazette, 47/2016.

4. CRITICAL INFRASTRUCTURE PROTECTION IN SERBIA

The Law on Critical Infrastructure Protection regulates national and European critical infrastructure identification and determination of the Republic of Serbia, competence and responsibility of authorities and organizations in the field of critical infrastructure and information, reporting, providing decision support, data protection, management and supervision in the field of critical infrastructure. In order for the Law to be fully applicable, the Regulation on the criteria for the critical infrastructure identification and manner of reporting it was adopted in the Republic of Serbia in 2022. The criteria according to which critical infrastructure is identified are determined based on the assessment of the consequences that may occur due to critical infrastructure disruption or destruction, as well as based on the consequences that may occur in the event of threats to critical infrastructure. The criteria

established by this regulation are the basis for determining critical infrastructure in the Republic of Serbia.

One of the main reasons for the adoption of the Law on Critical Infrastructure (“The Official Gazette of the Republic of Serbia”, 87/2018) is the absence of a single law in this area and the need to unify it. The term ‘critical infrastructure’ is mentioned in several different documents, first of all, in the Law on Emergency Situations, then in regulations and strategies, but also in the Law on Information Security and the Law on Private Security. The law first defines the terms included in the content, starting with what the critical infrastructure sector is, then the way in which identification, determination, protection is carried out, who the operators are, what the security plan, is liaison officer and finally what European critical infrastructure is. The principles of action contained in this Law apply to competent authorities, organizations and citizens, and these subjects are obliged to comply with them. The principles are exhaustively enumerated in the Law, namely the principles of integrated approach, responsibility and protection against various types of threats, the principles of continuous planning for critical infrastructure protection, data and information exchange and data protection (Micovic, 2020).

Of course, the newly adopted law has been harmonized with the EU directives concerning critical infrastructure, while retaining a certain independence in defining critical infrastructure and the way of responding to its threat. Some of the laws concerning critical infrastructure are: the Law on Railways (“The Official Gazette of the Republic of Serbia”, no. 41/2018); the Law on Safety in Railway Traffic (“The Official Gazette of the Republic of Serbia”, no. 41/2018); the Law on Interoperability of the Railway System (“The Official Gazette of the Republic of Serbia”, no. 41/2018); the Law on Electronic Communications (“The Official Gazette of the Republic of Serbia”, no. 44/2010, 60/2013 – Constitutional Court Decision, 62/2014 and 95/2018 and other laws); the Law on Water (“The Official Gazette of the Republic of Serbia”, no. 30/10, 93/2012 and 101/2016); the Law on Meteorological and Hydrological Activities (“The Official Gazette of the Republic of Serbia”, no. 88/2010); Strategy for Electronic Communications Development (“The Official Gazette of the Republic of Serbia”, no. 68/10); the Law on Electronic Document, Electronic Identification and Trust Services in Electronic Business (“The Official Gazette of the Republic of Serbia”, no. 94/2017); the Law on Electronic Commerce (“The Official Gazette of the Republic of Serbia”, no. 41/2009 and 95/2013); the Law on Confirmation of the Convention on High-tech Crime (“The Official Gazette of the Republic of Serbia”, no. 19/2009); the Law on Private Security (“The Official Gazette of the Republic of Serbia”, no. 104/13); the Law on Organization and Competence of State Bodies for the Fight against High-tech Crime (“The Official Gazette of the Republic of Serbia”, no. 61/2005 and 104/2009); the Law on Information Security (“The Official Gazette of the Republic of Serbia”, no. 6/2016 and 94/2014); the Law on Data Confidentiality (“The Official Gazette of the Republic of Serbia”, no. 104/2009). The methodology and contents of the disaster risk assessment and the protection and rescue plan were published in “The Official Gazette of the Republic of Serbia”, no. 87/2018.

Critical infrastructure existence and protection is nothing new to the Republic of Serbia, as it has been dealing with this issue successfully for many years, especially in the part where critical infrastructure can be threatened by natural disasters and various accidents. By introducing the new law, Serbia only “unified” numerous provisions related to critical infrastructure, which were defined in some other laws.

5. CRITICAL INFRASTRUCTURE PROTECTION IN BOSNIA AND HERZEGOVINA

When it comes to critical protection infrastructure in Bosnia and Herzegovina, with its entities and Brcko District, has not yet done anything, nor are there any indications that much will happen in the near future. Bearing in mind that Bosnia and Herzegovina shares similar critical infrastructures with its neighboring countries, as well as the causes of threats to critical infrastructures, it is clear that quality legal solutions and their application in practice can be reached in a short time. The reason for the absence of quality response as far as Bosnia and Herzegovina is concerned, can be found in political misunderstanding or lack of desire to protect critical insurance approaches in the optimal and recommended way. One of the reasons, but not the main one, is the way Bosnia and Herzegovina is organized and functions. Brcko District has no adopted documents related to critical infrastructure protection, and neither does the Federation of Bosnia and Herzegovina. In the Republic of Srpska, the situation is somewhat more favorable. There is an adopted law, but nothing further has been done in accordance with that law. The Law on Critical Infrastructure Safety in the Republic of Srpska, was adopted in 2019 (The Official Gazette of the Republic of Srpska, no. 58/19). That there was no further implementation of the Law is evident from the following:

- According to the provisions of this Law, Government of the Republic of Srpska was obliged to pass a bylaw regulation on the procedure for checking the critical infrastructure subjects and facilities with six months from the date of this Law entering into force – it was not done;
- According to the provisions of the law, the heads of the Republic’s administrative body were obliged to adopt certain sectoral measures within eighteen months form the date of this Law entering into force – it was not done;
- According to the provisions of the law, Ministry was obliged to adopt the sectoral measures to adopt Methodology which would refer to critical infrastructure^a within nine months from the date of this Law entering into force;
- According to the provisions of the law, the republic’s administrative bodies were obliged to propose critical infrastructure from their jurisdiction’s sector and their level of criticality, within six months from the Methodology adoption date – it was not done.

If the Law were to be implemented now, the effect would certainly be very weak. This is due to the fact that the five-year cycle since the adoption of the law is coming to an end, i.e., the period when everything done so far should be reviewed. The audit would give a special review of the effectiveness of the measure applied to critical infrastructure facilities, thus creating preconditions for a possible change in the existing legal solutions, The lost time and failure to understand the need to protect critical infrastructure in Bosnia and Herzegovina only shows that the society as a whole is not ready to accept and respond to the need to protect critical infrastructure, and thus, in addition to its own community, it also puts neighboring countries in a disadvantageous situation. Due to this attitude towards the critical infrastructure protection, neighboring countries will have to engage additional resources in order to prevent

^a The methodology was done by Ministry of the Interior of the Republic of Srpska and in cooperation with the Civil Protection Republic Administration, but it was graded with a certain degree of secrecy. The essential question relates to the reasons for “secrecy” for the methodology used. The methodology that refers to critical infrastructure protection or is directly related to critical infrastructure facilities in neighboring countries is a publicly published document in The Official Gazette and publicly available to everyone. Author’s comment.

the threatened infrastructure in Bosnia and Herzegovina from “spilling over” onto their countries as well.

7. CONCLUSION

The adoption of measures and their redefinition regarding the identification and critical infrastructure facility protection measures clearly indicate social awareness development of the need for mutual action, very often at the regional level, in order to be able to speak with certainty about its protection readiness in all circumstances. Croatia, as a member of the EU, adopted the Law that fully implements the EU Directive 2008/114/EC, while respecting the specificities at the national level. Serbia, even though it is not a member of the EU, accepts the mentioned Directive, and it can be said that it regulates the legal solutions related to critical infrastructure in a better way. This is a consequence of constant change monitoring in a country and environment that may affect critical infrastructure, as well as many years of experience in this field. Bosnia and Herzegovina, by not adopting any documents, at the level of the Council of Ministers, districts or entities, only complete a general picture that indicates that Bosnia and Herzegovina is a creation that is not able to take care of elementary things that should be in its/their jurisdiction. This inert attitude puts the neighboring countries in a disadvantageous position. Namely, in addition to managing the state of their critical infrastructures, they are “forced” to think about the same in Bosnia and Herzegovina. This is due to the fact that it is expected that the critical infrastructure threat in any part of Bosnia and Herzegovina, due to an inadequate response, may spread to the neighboring countries’ territory

REFERENCES

Kekic, C. (2019). Direktiva Saveta o utvrđivanju i označavanju evropske kritične infrastrukture i proceni potrebe unapređenja njene zaštite. Evropsko zakonodavstvo, Institut za međunarodnu politiku i privredu, Beograd.

Milosavljevic B., Komazec N. (2021). Kritična infrastruktura i društvena odgovornost, Istraživački centar Banja Luka, Zbornik radova, „Zastota kritične infrastrukture-obaveze država i mogućnosti privatnog sektora bezbjednosti“, Naučno-stručna konferencija sa međunarodnim učešćem, Banja Luka.

Micovic, M. D. (2020). Specifičnosti kritične infrastrukture u Republici Srbiji. (Elektronski izvor).

Istraživački centar Banja Luka. (2021). Zbornik radova, „Zastita kritične infrastrukture-obaveze država i mogućnosti privatnog sektora bezbjednosti“, Naučno-stručna konferencija sa međunarodnim učešćem, Banja Luka.

Narodne novine Republike Hrvatske broj 47/2016

Službeni glasnik Republike Srbije broj 87/18 i 69/22

Službeni glasnik Republike Srpske broj 44/2010, 60/2013, 62/014, 95/2018, 87/201841/2018, 58/19.

<https://federalna.ba/nato-i-eu-pokrecu-radnu-grupu-za-zastitu-kriticne-infrastrukture-isulo>
NATO i EU pokrecu radnu grupu za zastitu kritične infrastrukture, Accessed: 11.01.2023.

THE CONCEPT OF TOTAL DEFENSE IN THE REPUBLIC OF SERBIA

Sladjana Eric^{1a}

¹ Human Resources Sector Ministry of defence, Bircaninova 5, Beograd, Republic of Serbia,
eric.sladjaja@gmail.com

Received: 25th August 2023

Accepted: 8th September 2023

Original scientific paper

Abstract: *At all levels of social development, there are trends of change and adaptation to the dynamic security environment. Defense systems based on solid foundations of national and collective security, along with monitoring the scientific and technological achievements of the modern age, see an equal need for revitalization as well as modernization of their potential. Traditional concepts of the defense system confirm their inviolability in the face of long-term crises even in the third decade of the 21st century. However, the success of the sustainability and reorganization of the defense system depends on the implementation of the results of the work of scientific and professional circles. The concept of total defense shown in the case study of the Republic of Serbia will describe the elements of the defense system common to all national states, but also the specifics of a comprehensive approach to the concept of total defense at the national level.*

Key words: *national security, defense, comprehensive approach to the concept of defense, military defense, civil defence*

1. INTRODUCTION

Seemingly overcome by the fear of a global conflict similar to the Second World War, and then by the bloc tensions characteristic of the Cold War period, they deny asymmetric threats such as terrorism, and in the second decade of the 20th century, the pandemic caused by the spread of the viral infection Covid-19 associated with the realignment of the main actors in multipolar world order.

Theoretical and practical viewpoints regarding security and defense have always been and remain current among scientific and expert circles, the academic public, and above all among political decision-makers. Although primacy is given to military defense in relation to other aspects of ensuring the survival of the population in a certain territory, any point of view about the self-sufficiency of military defense is doomed to failure at the start.

Since the 6th century, official attention has been paid to the unarmed aspect of defense, defense by non-military means or civil defense in international law, strategic determinations of national states, as well as doctrines of military-political alliances. Strategic and indoctrinated

^a ORCID: 0009-0000-9432-3553

documents, and then international and national regulations conditioned the obligation, primarily, of state actors to plan, build, and even to arrange and adjust existing capacities and infrastructure in order to support the concept of civil defense. The attempt to systematize knowledge from political, economic, sociological, and above all security and military sciences, in order to build a stable and functional civil defense system, is given priority ad hoc. More dominant and frequent were the determinations of the national states to partially observe the concept of civil defense or bring it together with military defense within the concept of total defense.

2. REVITALIZATION OF THE CONCEPT OF TOTAL DEFENSE

The revitalization of the concept of total defense is significantly influenced by predictions of security risks and threats. Taking into account the past experiences in the implementation of a comprehensive approach to defense, and above all the experiences of countries that based the realization of national defense on collective defense, one constant can be observed in the indisputable confirmation of the importance of the concept of total defense.

When considering the state strategic commitments, it should always be borne in mind that their strategic documents in the field of security and defence are most often changed with the change of the strategic (security) environment, primarily in the case of states that are within certain collective security systems (e.g. NATO members), which generally does not apply to militarily neutral and other politically and economically independent states (Golubovic & Sakovic, 2023).

The readiness to defend the country and the support of the citizens in defense efforts are key factors in building a credible defense. Citizens and decision makers must be aware of what crisis and war conditions require of them.

Modern concepts of comprehensive national defense are based on two basic principles - resistance and resilience. Resistance refers to the will and readiness to defend the country in case of military threats. Resilience refers to the willingness of civilians to maintain the functioning of society in the event of a crisis, including a military attack (Berzina, 2020).

As some authors point out, in their security and defense policy documents, many states and international organizations (EU, NATO, etc.) have defined a comprehensive approach to the defense of national interests and adapted their doctrinal frameworks accordingly. Total defense is the combined efforts of the military services, relevant civilian agencies, and various societal actors, including businesses, in the face of an armed aggression from abroad (Bengt & Jan, 2023).

Depending on the way components (entities) are organized and available resources are managed, theoretically and practically different defense models can be distinguished. Some authors mention two models:

- territorial model based on the territorial-administrative organization of the state i
- a functional model that starts with functional organization in relation to the important dimensions of a society (Berisa, 2017).

One cornerstone of the old total defense concept was the will to defend, which included popular support for preparedness for crises and war (Bengt & Jan, 2023).

Total defense is planned, organized and implemented in peace, state of emergency and war, by engaging part or the entire defense system in the protection and realization of the defense interests of the Republic of Serbia. Some of the basic assumed success of total defense can be considered: timely and comprehensive preparations of all subjects of the defense system;

planned, organized and timely mobilization; favorable strategic and operational development; organized territory; unified, coordinated and determined action of all defense forces; motivation for defense and resistance and others. The basis for the preparation and implementation of total defense is reliance on one's own potential, which does not exclude cooperation with other countries and international organizations.

3. CIVIL DEFENSE

Aimed at protecting the state as a reference object, security "providers" are faced with the challenge of constant adaptation to the security environment. Civil defense is one of such "providers" of security, whose bearers, in the Republic of Serbia, are all relevant segments of society, which are defined in the broadest sense as state bodies, bodies of autonomous provinces, bodies of local self-government units, companies, other legal entities and entrepreneurs, and even citizens in an organized and regulated sense with precisely defined rights and obligations. In a narrower sense, we can look at "providers" of security embodied in the form of civil defense according to their territorial coverage; levels of jurisdiction; the degree of exposure to security challenges, risks and threats from which they should protect the population in a certain territory and others. Regardless of how you define civil defense, in a narrower or broader sense, the tasks and activities of civil defense, as well as the bearers of their implementation, are integrated by the Ministry of Defense. This coordinating role of the Ministry of Defense in the field of civil defense is reflected in peacetime conditions through the preparation of the subjects of the defense system for action in conditions of emergency and war, while in the case of declaration of a state of emergency and war, the competence of the Ministry of Defense is to direct the subjects to act according to the documents for the implementation of the Plan defense of the Republic of Serbia. The purpose of civil defense is to protect the state and the population from dangers that come as a result of armed conflicts, but also in major emergency situations of a natural and man-made nature (Valjerjevic & Mladenovic, 2018). In accordance with strategic objectives, effective civil defense contributes to the protection of the sovereignty, independence and territorial integrity of the Republic of Serbia. Normative-legal regulation of civil defense, in accordance with the concept of total defense, will specify competences, increase responsibility and improve the competence of subjects of the defense system in the field of civil defense. The Republic of Serbia will advance preparations for civil defense. Special attention will be paid to building organizational capacities for unified management of civil defense, and organizational and personnel capacities for training all subjects of the defense system. Normative and legal regulations related to civil defense will also be updated, as part of the defense of the Republic of Serbia. Special attention will be devoted to the training of the population for defense, and the development of coordination mechanisms of the subjects of the defense system (Strategija odbrane RS, 2019).

Civil defense should fulfill tasks in accordance with the code of international humanitarian law, especially those related to: prevention and opposition to all forms of threats to people, material goods and the environment; organization and functioning of state authorities; organization and functioning of the economy; organization and functioning of public services of special importance; protection and rescue of the population and material goods (Komazec et al., 2016).

4. SYNERGY OF VITAL COMPONENTS OF TOTAL DEFENSE

The application of total defense enables the defense system to be engaged in a comprehensive and unique way, which implies the integral engagement of all subjects of the defense system and the defense potential of a state. Given the specifics of the entities and defense forces, total defense includes military and civilian defense. Military defense is focused on preparation for

defense and defense of the use of the army and other armed forces of defense. Civil defense, as a part of defense, is limited to preparations for defense and defense by non-military means. Between military and civil defense, it is easy to learn and inevitably implies a causal connection.

The development of military defense is coordinated with the development of the defense system of the Republic of Serbia. Military defense preparations are carried out continuously, comprehensively and planned, in order to maintain a high degree of combat readiness. Qualitative and quantitative features of military defense certainly constitute the military power of the state. Military defense is focused on preparations for defense and defense using the army and other armed forces of defense. The security logic that dominates official discourses emphasizes total defense against military and nuclear attacks; or focusing on crisis preparedness practices when the military threat is no longer imminent; or an attempt to combine both approaches when a military threat is again possible (Wrangle, 2022).

In former "total" wars, the military imperative permeated all areas of social action. Developed capabilities for countering military threats will also enable participation in countering or removing the consequences of non-military threats while providing support to civil authorities. Taking into account the uncertainty and changed physiognomy of future multidimensional security challenges, risks and threats, the defense system needs to develop a wide range of capabilities that enable responses of both a military and non-military nature. The whole society must be resistant to the danger of the 21st century, and the activities must function even when the society faces difficult challenges and crises. People must have access to the most basic - food, water, electricity, transportation, education and upbringing of children and other things, and it is precisely the basic task of the civil defense system to enable the functioning of all the mentioned activities.

Ensuring the implementation of military defense and civil defense in conditions of emergency and war is the function of protecting national values and interests with unarmed means of defense.

5. CONCLUSION

At the global level, military confrontations are certainly the primary source of instability, while each subsequent year of human development implies the modernization of military equipment and weapons with the application of modern models of warfare. Therefore, it is expected that future classifications of security challenges, risks and threats will be subject to revision, primarily in terms of supplementing newly discovered or modified threats. The pandemic caused by the viral infection Kovid-19 reminded the entire humanity of the need to revive the non-military aspects of defense. The war in Ukraine, but also other smoldering hotspots, primarily on the European, Asian and African continents, along with the acquisition of weapons of mass destruction, would represent an alarming threat to the survival of the entire planet. In addition, the exhaustion of renewable and non-renewable resources, combined with natural disasters, the causes of which are mainly climate change, reminds us that something urgent must be done.

Whether humanity will be able to predict the future and what will be the ability to adapt to the upcoming changes, certainly remains an open question for both current and younger generations. The pursuit of the sustainability of the concept of total defense is both a new and an old "philosophy" on which nation-states rest. The challenge for political actors, as well as the entire social sector, is the ability to create human resources who clearly know and act in accordance with their knowledge and skills in the context of the total defense of national interests.

REFERENCES

- Berisa, H. (2017). Aspekti koncepta totalne odbrane. Integralna bezbednost Republike Srbije: teorijski aspekt, Fakultet za poslovne studije i pravo i Fakultet za strateski i operativni menadzment Univerziteta – Union “Nikola Tesla”, 978-86-87333-74-1, Beograd.
- Berzina, I. (2020). From ‘total’ to ‘comprehensive’ national defence: the development of the concept in Europe, *Journal on Baltic Security*, 6 (2).
- Golubovic, M. Sakovic, R. (2023). The comparative analysis of the state strategic documents in the field of security, *Vojno delo*, 1/2023, pp. II/1-II/17, 0042-8426.
- Komazec, N. Soskic, S. Karapetrovic, Lj. (2016). Civil defense and protection in crisis management system, The Second International Scientific and Professional Conference “Safety and Crises Management– Theory and Practice”, Ivanis, Z. Babic, B. Komazec, N. (Ed.) pp. 16-22, 978-86-80698-01-4, Obrenovac, September 2016, Regional association for security and crisis management, Belgrade.
- Strategija odbrane Republike Srbije (2019). Sluzbeni glasnik RS broj 94 od 27. decembra 2019. godine” Available from [http://www.parlament.gov.rs/upload/archive/files/cir/pdf/ostala_akta/2019/220719%20\(RS60\).pdf](http://www.parlament.gov.rs/upload/archive/files/cir/pdf/ostala_akta/2019/220719%20(RS60).pdf) Accessed: 24.06.2023.
- Sundelius, Bengt. Eldeblad, (2023). Societal Security and Total Defense: The Swedish Way, *Prism*, 10 (2).
- Valjerjevic, V. S. Mladenovic, M. (2018). Civilna odbrana u sistemu nacionalne bezbednosti Ruske Federacije, *Godisnjak Fakulteta bezbednosti*, 2018.
- Wrange, J. (2022). Entangled security logics: from the decision-makers discourses to the decision-takers interpretations of civil defence. *European security*. 31 (4).

EMERGENCY HEADQUARTER`S „TABLE TOP” EXERCISES IN LOCAL GOVERNMENTS

Dragisa Jurisic^{1a}

¹ Security Research Center, Street Sinise Mijatovica 9, Banja Luka, Republic of Srpska,
Bosnia and Herzegovina, bicbl@yahoo.com

Received: 5th August 2023

Accepted: 16th August 2023

Review paper

Abstract: *Emergency management requires teamwork within the structures that manage responses to them. In order to achieve that teamwork, it takes a lot of time, joint work, and good mutual knowledge of staff members. This implies the need for joint training in procedures, activities, exchange of information, etc. Preparations for exercises often take a lot of time, and the implementation itself is long and complex. In addition, there are other reasons for not implementing exercises and training, and most often it is money, which is lacking for this type of activity at the level of local self-government units. All this leads to the fact that local self-government units avoid carrying out exercises of protection and rescue forces. This work should show that "table top" exercises are an ideal tool for training staff for emergency situations at the level of local self-government units and that they enable team building and staff cohesion, which is of great importance in emergency situations. Moreover, only goodwill is needed to prepare, organize and implement this type of exercise.*

Key words: *„table top” exercises, local governments, headquarters, emergency, training*

1. INTRODUCTION

In 2022, the Emergency Event Database - EMDAT recorded 387 natural hazards and disasters worldwide, resulting in the loss of 30,704 lives and affecting 185 million individuals. Economic losses totaled around 223.8 billion US\$. (EMDAT, 2023) It shows that natural hazards represent a great challenge for all countries of the world.

The listed data show that the threat from natural or other dangers is constant and that it is necessary for the training and qualification process to be constant, which ensures the complete and accurate execution of tasks. Civil protection as the bearer of the protection and rescue system to emergency situations, in order to function effectively and perform its functional tasks, must be supported by an effective process of training. Training is one of the key factors in good emergency response preparedness.

^a ORCID: 0000-0002-7225-0493

Regarding training, Sendai Framework for Disaster Risk Reduction proposes improving the knowledge of services at all levels, civil society, community, and volunteers, as well as the private sector, by sharing experiences, lessons learned, good practices, and training and education on disaster risk reduction, implementing the application of existing training and education mechanisms. According to that the members of the protection and rescue system are trained through courses, seminars, trainings, and exercises. These activities provide an opportunity to test the system, identify deficiencies and improve efficiency in responding to crises.

One of the best tools to prepare people for response in case of natural or other disasters is different kinds of exercises. The exercises are practical activities to improve your skills. It is that kind of training where it is possible to train individuals, units, and headquarters to perform practical activities in the case of natural disasters. Also, the exercises can be used for:

- testing and verification of policies, plans, procedures, training, equipment, interagency agreements,
- clarification and training of staff for certain roles and responsibilities,
- improving coordination and communication between agencies,
- improvement of individual performance,
- identifying gaps in resources and
- identifying areas for improvement (FEMA, 2020).

In general, exercises can be divided in order of increasing organizational intensity and investment into:

- Discussion or seminar platforms designed to provide information on procedures and organizational plans.
- “Table-top” exercises (TTX) are designed to engage participants in real situations to understand and imagine the application of procedures.
- Command post exercises that typically involve lead communication and coordination personnel in simulated incidents conducted in actual command post facilities.
- Live field exercises that allow organizations to test responses in real-world situations (Prior & Roth, 2016).

This paper will try to show, that TTX, is an ideal tool for training civil protection headquarter staff for emergency situations at the level of local self-government units. Also, TTX enables team building and staff cohesion, which is of great importance in emergency situations, and on the other hand, only goodwill is needed to prepare, organize and implement this type of exercise. Moreover, there will be shown that BiH civil protection institutions, and in this work especially civil protection elements in towns of BiH, do not use enough or at all those TTX to improve their capability.

2. TRAINING OF CIVIL PROTECTION IN BiH

The protection and rescue system in BiH is organized so that its holders are the entities (Republic of Srpska and Federation of BiH), and the state level of BiH has the role of coordinator, and therefore the activities in the field of training in the field of protection and rescue have certain specificities. In order to manage this coordination at the BiH level, the Department for Protection and Rescue was formed within the Ministry of Security of BiH.

In accordance with the Framework Law on Protection and Rescue, the training of protection and rescue forces is exclusively under the jurisdiction of the entities. (Official Gazette BiH, No 50/08) In article 14 of the same Law, the Ministry of Security "in cooperation with entity administrations of civil protection", and not independently, organizes, among other things, exercises of international importance, that is, entities and Brcko District BiH are independent in terms of training and exercises of their own protection and rescue forces.

From 2019 until 2022, the "Manual for Planning, execution, and evaluation of protection and rescue exercises in Bosnia and Herzegovina" was developed. The purpose of this manual is to define a unique methodology for planning and implementing exercises, from the level of the local community to the level of state institutions, as well as for exercises with different numbers of participants. The entities and Brcko District BiH accepted to use this manual.

After the big floods of 2014 in BiH, the analysis showed that in BiH it is necessary to further develop protection and rescue systems with the assurance of continuous training and certification of individuals and organizations for planned and coordinated action in case of natural disasters.

Likewise, the general conclusions and recommendations of the Regional Conference "Floods in Southeastern Europe - lessons learned and further steps", regarding the floods of 2014 in BiH, state that training facilities of the highest standards do not exist in Bosnia and Herzegovina, and the existing capacities do not meet the required criteria. (Floods in Southeastern Europe, 2014) Also, the report from the NATO EADRCC exercise "Bosnia and Herzegovina 2017" clearly shows the shortcomings in the training of the protection and rescue forces. (EADRCC, 2017)

In the Republic of Srpska, the legal framework exists, but it has not been fully implemented for eleven years. The training system of protection and rescue forces is aimed at specialist units at the level of the Republic Administration for Civil Protection through various foreign projects while training at the level of local self-government units is left to them, and also there is no quality analysis and financial support for exercises at all levels.

Moreover, in the Federation of Bosnia and Hercegovina, in accordance with the "The Development program for the protection and rescue of people and material goods from natural and other disasters in FBiH from 2021-2028.", the current situation in the field of planning and execution of most forms of training is based on an *ad hoc* system on all levels from Federation over Cantons to local communities (FUCZ, 2021).

3. TABLE-TOP EXERCISE

TTX is used as a type of exercise in many organizations. All members of the Euro-Atlantic Partnership Council use the same Guidelines for planning, conducting, and assessment of international exercises where the TTX is one of the exercises. (EAPC(SCEPC)N(2009)0032-REV1, 2009) The Russians do not recognize TTX but they have exercises for training of personnel and they are similar to TTX (Методические, 2021). The last manual that was adopted at the BiH level in 2022, "Manual for planning, execution, and evaluation of protection and rescue exercises in Bosnia and Herzegovina" also foresees TTX (Prirucnik, 2022).

TTX is an exercise based on discussions and is one of the simplest types of exercises to implement. It is usually carried out indoors using office spaces where people work or which are provided for the purposes of the exercise. Conference or sports halls can be used for this type of exercise, depending on the size of the exercise and the number of engaged participants. Since these exercises do not involve the deployment of personnel and equipment on the field

and since there is no need for any special spatial capacities, these exercises are a flexible and economical way of training and exercise for civil protection headquarters.

These exercises are a cost-effective way of training in leadership and decision-making procedures in the context of emergency preparedness, which allows for avoiding some of the challenges of planning exercises in the field with real forces. In these exercises around the table, one tries to use real possible situations, which are used to start a discussion, check the procedures, start a discussion about the regulations, or draw a lesson and the best approach and way of acting in given situations. Moderators of exercise are responsible for presenting the problem, moderating the discussion, and sticking to the schedule.

The participants in TTX are decision-makers, planners, and managers, that is, leaders of certain units that participate in protection and rescue. These are exercises of headquarters not units.

According to some researchers there are some advantages and disadvantages of TTX.

- Requires only a modest commitment in terms of time, cost, and resources.
- Is an effective method for reviewing plans, procedures, and policies.
- Is a good way to familiarize key personnel with their roles and responsibilities.
- Is an opportunity to build trust (team building).
- It stimulates thought processes.
- Helps focus the team within a specific situation (scenarios such as cyber)
- Helps identify any issues, challenges and / or assumptions.
- Helps identify resources necessary to overcome any issues, challenges and/or assumptions.
- Helps identify means of overcoming any identified issues, challenges and/or assumptions.
- An opportunity for leaders to practice their crisis management leadership skills (Burton, 2020).

Also, the TTX are performed in a safe learning environment where participants can apply the theory of their policies and procedures to ensure they are fit for purposes..

Some of disadvantages of TTX are:

- Lacks realism and thus does not provide a true test of a crisis, emergency, security or business continuity management system's capabilities.
- Provides only a superficial exercise of plans, procedures, and team capabilities.
- Does not provide a practical way to demonstrate system overload (Burton, 2020).

However, if the TTX is poorly prepared and managed or unchallenging then the participants may get a false sense of readiness.

4. METODOLOGY

For the purpose of this research, a simply questioner was constructed and delivered to 33 towns (they have the status of the town) in Bosnia and Herzegovina, in order to get answers from them. An e-mail with questioner consisted also explanation, what TTX is, and how supposed to be executed, and all in order to make it easier for the responders. The questions were:

1. Have you implemented "table-top" exercises for the training of the Headquarters for emergency situations so far?
2. If yes, how many times in the last five years?
3. If yes, who prepared, organized, and executed that exercise?
4. How do you rate this type of exercise? Excellent, very good, good, bad
5. The reason why you think that these types of exercises deserve that rating? (Please explain in a few sentences!)

Moreover, the questionnaire was a very simple one, in order to avoid a problem collecting information, and depending on my previous experiences in working with civil protection in the local communities.

This questionnaire was sent by an e-mail to civil protection offices in the town's administration, if an e-mail address was available, and where it was not case e-mail was sent to the mayor's office or to some other addresses in the administration of the towns.

The results of this questionnaire were analyzed and some conclusions were driven from it.

5. DISCUSSION

At the beginning of this discussion is necessary to highlight that the questionnaire for this research was repeated twice in two months and just nine replies were received. It showed that local communities are not professional, or they are not willing to participate in this research. Simply there was not any reply from 24 towns. Also in that context, it is important to highlight that in those towns, that were contacted, just in twelve towns there was an e-mail for civil protection. In eleven towns e-mails were available only for the town's administration and in ten cases e-mails were personalized.

Towns were chosen to get questionnaires because of their complexity, population, and challenges that they have when it comes to natural or other hazards. The civil protection organization is supposed to be on a higher level, than in small municipalities. The Headquarters of civil protection at the town level is supposed to be complex, with a lot of members and different organizations, IOs, or NGOs, too. For them, TTX is a tool that they are supposed to use very often in their training.

In the end, the answers were got from six towns in Federation BiH (Lukavac, Gradacac, Mostar, Orasje, Sarajevo, Srebrenik) and from three towns in the Republic of Srpska (Gradiska, Prijedor, Banja Luka). Taking into consideration that there were just nine answers the analysis was conducted for each of them.

An interesting answer has come from Town Sarajevo in Federation BiH. According to the answer, in the Statute of the Sarajevo Town civil protection is not in the scope of work. It is the reason why they did not conduct TTX up to now. It is a quite strange answer and situation that a town with 400.000 inhabitants does not have civil protection in the scope of the work.

Also, the Town of Mostar responded that they did not have TTX up to now but they had civil emergencies, and the "headquarters of civil protection was performing well." Because of that, the people from Mostar's civil protection think that they do not need TTX training for Civil Protection Headquarters.

Banja Luka, as the biggest town in the Republic of Srpska, in the last ten years organized one TTX as part of the UNDP project. Members of the UNDP team prepared, organized, and realized the exercise, and in town civil protection graded it as "good" but they recognized the

importance of those TTXs and they thought that TTX should be in the civil protection plans regularly. The main reasons why the TTX is not now in plans are the “unwillingness of decision-makers and members of staff to be trained and qualified for emergency management, decision-making, and group decision-making. Another reason for not holding such exercises is the absence of supervision over the work of the headquarters.”

Prijedor's civil protection also did not have TTX but they answered that members of Civil Protection Headquarters should have TTX. The main reasons why it is not the case are the will to prepare, organize and conduct TTX, finances at the local community, and Law on civil protection should be revised.

The civil protection from Gradiska town also did not have TTX up to now and explanation is: "The reason for not holding the training is multi-layered and difficult to explain".

The Town Gradacac civil protection answered that they did not have TTX in the last five years but there was TTX 15 years ago, and Federal Administration for Civil Protection organized and conducted that TTX. The general attitude is that all exercises are useful and should be applied continuously.

Lukavac's civil protection also did not have TTX up to now and the reason for that is "insufficient interest or lack of information".

6. CONCLUSION

As was shown earlier, continuous education and training for all stakeholders of civil protection are vital to improving skills, knowledge, and emergency management capabilities. However, according to the answers to the questionnaire, it is quite clear that TTXs are not on the list of activities in the civil protection local community's plans. All nine towns that answered the questionnaire responded that they did not have TTX in the last five years. Some representatives of civil protection in towns were interested in TTX, and they had a positive attitude toward those exercises.

The main reasons why those TTX were not conducted were different but can be presented through “insufficient interest or lack of information”.

TTXs should be better presented to local communities because they are simple, not long-lasting, and cheap way of training. All those advantages of TTX can be used to improve the protection and rescue system on all levels of civil protection in BiH, especially at the local level.

REFERENCES

Burton, R. (2020). Tabletop Exercise – Pros and Cons, Available from <https://preparedex.com/tabletop-exercise-pros-and-cons/> Accessed: 26.07.2023.

EADRCC. (2017). EADRCC exercise report BiH2017, Available from <https://natohqgeo.maps.arcgis.com/apps/Cascade/index.html?appid=52c8272841e44fe4b620ce857a6581fe> Accessed: 2023-06-10.

EMDAT. (2023). 2022 Disasters in numbers: Climate in action, Available from https://cred.be/sites/default/files/2022_EMDAT_report.pdf Accessed: 12.05.2023.

FEMA. (2020). Homeland Security Exercise and Evaluation Program, Available from <https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep> Accessed: 27.06.2023.

Floods in Southeastern Europe - lessons learned and further steps. (2014). Available from https://www.racviac.org/wp-content/uploads/2022/02/IRC-12_overview.pdf, Accessed: 22.06.2023.

Framework Law on Protection and Rescue, the training of protection and rescue forces is exclusively under the jurisdiction of the entities. 2008. Official Gazette BiH, No 50/08.

EAPC(SCEPC)N(2009)0032-REV1. (2009). Guidelines for planning, conduct and assessment of international Euro-Atlantic Partnership Council exercises, Available from <http://www.msb.gov.ba/PDF/docEN30102015.pdf> Accessed: 16.06.2023.

Prior, Tim. Roth, Florian. (2016). Learning from Disaster Events and Exercises in Civil Protection Organizations, Risk and Resilience Report, Center for Security Studies (CSS), ETH Zurich, pp.17. Available from <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/RR-Report-2016-01%20.pdf> Accessed: 25.06.2023.

Prirucnik za planiranje, izvodjenje i evaluaciju vjeZbi zastite i spasavanja u Bosni i Hercegovini. (2022). Ministarstvo bezbjednosti BiH.

FUCZ. (2021). Program razvoja zastite i spasavanja od prirodnih i drugih nesreca u Federaciji Bosne i Hercegovine od 2021.- 2028., Available from <http://www.fucz.gov.ba/program-razvoja-zastite-i-spasavanja-od-prirodnih-i-drugih-nesreca-u-federaciji-bosne-i-hercegovine-od-2021-2028-godine/> Accessed: 03.08.2023.

Методические рекомендации по подготовке и проведению учений и тренировок по гражданской обороне, защите населения от чрезвычайных ситуаций природного и техногенного характера, обеспечению пожарной безопасности и безопасности людей на водных объектах. (2021). Available from <https://rulaws.ru/acts/Metodicheskie-rekomendatsii-po-podgotovke-i-provedeniyu-ucheny-i-trenirovok-po-grazhdanskoy-oborone,-zasch/> Accessed: 01.04.2023-04-01.

THE POSSIBILITY OF USING AN AIRBAG AS AN ALARM FOR INJURIES AT WORK

Predrag Vasiljevic¹, Milorad Danilovic^{2a}, Slavica Antonic^{3b}

¹ Forest farm "Severni Kucaj" Kucevo, Trg Veljka Dugosevica 26, Kucevo, Republic of Serbia, dragorad@gmail.com

² Faculty of Forestry, University of Belgrade, Kneza Visislava 1, Belgrade, Republic of Serbia, milorad.danilovic@sfb.bg.ac.rs

³ Faculty of Forestry, University of Belgrade, Kneza Visislava 1, Belgrade, Republic of Serbia, slavica.antonc@sfb.bg.ac.rs

Received: 7th August 2023

Accepted: 1th September 2023

Professional paper

Abstract: Chest injuries are rare but extremely life-threatening and can occur in all industries. Although popular belief is otherwise, most injured persons can be saved by appropriate surgical treatment. Thanks to the use of airbags as an alarm for workplace injuries, an injured worker can notify nearby colleagues without being aware of it. This alarm is triggered when the load exceeds 15 kilograms or when there is a loss of pressure in the airbag, indicating a strong impact in the body region where the airbag is located. In an enclosed environment, a receiver is located inside or outside the work area that responds to this alarm and alerts other workers to an injury that occurred through visual and audible signals. Airbags as workplace injury alarms can be used successfully in a variety of fields and work environments, particularly in forestry, agriculture, mining, construction, and machine room operations.

Key words: injury at work, chest, alarm, airbag

1. INTRODUCTION

Although the most frequently injured parts of the body of forest workers are the extremities such as legs (34%), arms and hands (26.9%), and then the head and neck area (15.2%) (Tsioras et al., 2014) injuries of the chest are not as common (about 7%) (Potocnik et al., 2009), but they are life-threatening. They occur in all industries, not only in forestry. However, forestry is one of the high-risk groups because it works in difficult terrain and with equipment that is often insufficient to protect the workers.

The most common chest injuries are: severe chest contusion, rib or sternum fracture, ruptured lung due to the sharp edge of a broken rib entering the lung, which may be the result of a lung puncture or a foreign object entering the chest, collapsed lung due splashing or bleeding, etc.

^a ORCID: 0000-0002-2509-6390

^b ORCID: 0000-0001-8835-1259

Contrary to popular belief, most injured people can be saved by appropriate surgical treatment. However, due to the above-mentioned injuries, the injured worker is often unable to ask for help promptly because he is in a state of shock or unconsciousness, which prevents him from requesting the fastest possible help.

Ibrahim et al. (2023) investigated the use of an airbag and signaling during falls in the elderly. This system can be attached to the waist belt like an airbag. It is wirelessly connected to the elderly person's cell phone, for which an Android mobile application was created to receive alerts from the system. The system detects the fall using a gravity sensor connected to the "Arduino board". When the gravity sensor detects a fall, the system activates the air valve and inflates the airbag from the air reservoir. The system then sends an alert via Bluetooth to the person's application, which is specified as the contact for the elderly person. Arduino boards are used for fall detection based on set threshold values (Manigandan & Norman, 2015).

This model was developed by Toshiy et al. (2009), who conducted studies on 16 subjects simulating a fall. They then developed a fall detection algorithm that could detect signals 300 ms before a fall. This signal served as a trigger to inflate the airbag to a capacity of 2.4 l.

Following a similar model, thanks to the use of an airbag as a workplace injury alarm, an injured worker can send a call for help to the adjacent group of workers without even being aware of it.

The aim of this work is to show the principle of operation and the possibility of using an airbag as an alarm for workplace injuries.

2. WORK METHODOLOGY

For the purposes of this work, a prototype was made that consists of several elements. These elements are: an airbag, a pressure sensor that processes the pressure difference and provides at its output a voltage signal ranging from 0 to 5 V, an electronic part that increases the input signal provided by the pressure sensor and sends a pulse to the transmitter of the remote part of the device through the input signal comparator, which has the task of turning on the receiver through radio signal that reports a possible injury to the worker.

The input signal, i.e. increasing the pressure in the airbag, represents the pressure of a foreign object on the chest, abdomen or part of the body most at risk in the workplace, a place with a high risk of injury. The receiver is located in the protective helmet of the worker of the adjacent group, which warns of possible injury to the worker by vibration and a light signal, on which the airbag with the alarm is placed. This concept refers to the workers who are in the field and do not have direct mutual communication due to distance, noise, work organization, etc.

In an enclosed space, the receiver that triggers the alarm is placed in the inner or outer part of the work area, where other workers are warned of the injury by a light and sound signal. On the circuit board of the electronic part, there are two potentiometers, with which we set the lower and upper air pressure thresholds, based on which the alarm signal is sent.

An alarm signal is also sent when the pressure in the airbag drops below the limit set on the potentiometer for the lower threshold. This means that there has been an injury, an impact with the sharp object, which has caused the airbag to burst.

3. RESULTS

In this work, the radio signal range was measured between the transmitter, which is connected to the airbag through an electric valve, and the receiver, which is located in the protective helmet and is connected to the vibration motor, which is firmly attached to the inside of the

protective helmet, and the LED which flashes when the alarm is activated and is located directly above the worker's eyes.

Based on the measurements, we came to the result that the ultimate range of radio waves between the transmitter and the receiver is up to 120 meters without concrete or metal obstacles, i.e. in an open space. Considering the fact that the working groups, for example in the construction industry, are located at a much shorter distance, the mentioned range is quite sufficient.

Measurements of the pressure exerted on the airbag were also carried out in order to trigger the alarm. The airbag is loaded with a weight of 15 kilograms, and this weight was sufficient to trigger an alarm to inform a worker in another workgroup or a light and sound signal in the workshop that an injury had occurred.

For the purpose of this work, the airbag was repeatedly loaded with a constant pressure of 15kg or more, and the prototype reacted at different pressures depending on the position of the weight itself, sending a signal of possible injury at work. The reason for the deviation from the value of 15 kg, which was set as the limit for triggering the alarm, is due to the fact that the airbag tends to deform, affecting the change in its internal pressure, which is the basis for triggering the alarm (table 1). Since a prototype was made for the purposes of this work, which is still in the testing phase, the measurements were not performed on a group of workers under different working conditions, but only experimentally.

Table 1. Measurement results (*Source: Authors*)

Measurement results												
Number of measurements	1	2	3	4	5	6	7	8	9	10	11	12
Prototype reaction (kg)	15.10	15.50	15.08	15.02	15.06	15.01	15.11	15.12	15.06	15.90	15.80	15.10
Average value (kg)	15.24											

In this prototype, we used potentiometer RV1 to set the lower threshold value and potentiometer RV2 to set the upper threshold value of the air pressure at which the alarm signal is sent. For the purposes of this work, the lower pressure threshold of the cushion is set to 140 mmHg or 0.187 bar, while the upper threshold is set to 250 mmHg or 0.333 bar. The pressure change sensor sends a 4.18 V signal at its output and triggers the alarm when the pressure in the airbag drops below 140 mmHg or 0.187 bar. If the pressure in the airbag reaches a value of more than 250 mmHg or 0.333 bar, the pressure sensor also sends a signal to activate the alarm. This means that an unplanned high pressure has occurred in the airbag caused by an injury, foreign object impact, contusion, etc.

An alarm is also triggered if the negative pressure in the airbag is below 140 mmHg or 0.187 bar. In this case, it is assumed that the airbag was punctured due to the penetration of a foreign object that caused the injury. However, if the worker suddenly faints and is unable to call for help, the worker himself triggers the alarm by releasing the safety valve, which causes the pressure in the airbag to drop below the lower threshold on the potentiometer RV1, which also triggers the alarm.

The voltage in the pressure sensor is directly and proportionally related to the pressure in the airbag. When the pressure in the airbag drops below 140 mmHg or 0.187 bar, then the voltage

in the pressure sensor drops below 4.18 V and the alarm is triggered. Likewise, when the pressure in the airbag rises due to a crush or impact and exceeds 250 mmHg or 0.333 bar, the voltage in the pressure sensor rises above 4.88 V and the alarm is triggered. These values are logical because the working voltage of the pressure sensor is from 0 V to 5 V (Table 2).

Table 2. Voltage and pressure when the alarm is activated (*Source: Authors*)

„Lower threshold“ of alarm activation	Safe zone	„Upper hreshold“ of alarm activation
Air sensor voltage	In this zone, the alarm activation is disabled because the parameters on the potentiometers for the "lower" and "upper threshold" of the alarm activation are set so.	Air sensor voltage
Alarm start		Alarm start
(V)		(V)
4,18		4,88
Airbag pressure		Airbag pressure
(bar)		(bar)
0,187		0,333
A millimeter of mercury		A millimeter of mercury
(mmHg)		(mmHg)
140		250

The safe zone, i.e. the range in which no alarm is triggered is between 140 mmHg and 250 mmHg, allowing workers to perform their jobs without triggering alarms unnecessarily. If a pressure of more than 15 kilograms is applied to the cushion due to crushing, in the airbag the pressure in the pressure sensor rises above 250 mmHg or 0.333 bar, the voltage rises above 4.88 V and the alarm is triggered.

4. CONCLUSION

The application of the airbag is suitable for use in different fields and for different purposes. In this work, it has been shown that it can be used as an alarm device for workplace injuries, especially in areas with a high frequency of injuries, such as forestry. It can be used especially in the exploitation of the forests, where the most common injuries occur during logging and wood products manufacturing, where bruises and impacts occur during tree felling.

The alarm is triggered not only in the event of a load of 15 kilograms or more but also in the event of a loss of airbag pressure, which means that there has been a strong impact in the area of the body where the cushion is located.

It should be noted that the use of such a device is also possible in economic sectors, where workers are often buried by earth collapses during the excavation of trenches, deep canals, etc. Due to the noise at the workplace and the medical condition of the injured worker, communication, i.e. calling for help, would be possible through this device, which would reduce the possibility of death after more serious injuries.

REFERENCES

Petros A. Tsioras, Christian Rottensteiner, Karl Stampfer, (2014). Wood harvesting accidents in the Austrian State Forest Enterprise 2000–2009, *Safety Science*, Volume 62, ISSN 0925-7535, <https://doi.org/10.1016/j.ssci.2013.09.016>.

PotoCnik, I., Pentek, T. i Poje, A. (2009). Severity Analysis of Accidents in Forest Operations. *Croatian Journal of Forest Engineering*, 30 (2), <https://hrcak.srce.hr/47892>

Ibrahim, M., Shawish, S., Aldroubi, S., Dawoud, A., Abdin, W. (2023). Airbag Protection and Alerting System for Elderly People. *Appl. Sci.* 13, 9354. <https://doi.org/10.3390/app13169354>

Manigandan, S., Norman, S.R. (2015). Fall detection system for elderly person monitoring using GSM network. *Int. J. Adv. Eng.* 1.

Toshiy, T., Senio, M., Takumi, Y., Masaki, S., Mitsuo, U., Osamu, T. (2009). A Wearable Airbag to Prevent Fall Injuries. *Eee Transactions On Information Technology In Biomedicine*, Vol. 13, No. 6.

PERSONAL DATA PROTECTION – FRAMEWORKS, PRACTICAL EXPERIENCES AND CHALLENGES

Radoslav Rakovic^{1a}

¹ Energoprojekt Entel plc, Belgrade, Bulevar Mihajla Pupina 12, Belgrade, Republic of Serbia, rrakovic@ep-entel.com

Received: 25th June 2023

Accepted: 7th August 2023

Review paper

Abstract: *Fundamental information security management standard ISO 27001 declares need for protecting basic features of information – confidentiality, integrity and availability - and defines certain number of controls oriented to technical, organizational and combined actions that should enable it. Particular issue represents personal data protection that is subject of particular General Data Protection Regulation (GDPR) has been applied in EU from 25.05.2018. and particular Law on personal data protection of Republic of Serbia has been applied from 22.08.2019. After brief review of the GDPR and the subject law, practical experiences and challenges in application of personal data protection in Serbia are considered.*

Key words: *information security, personal data protection, general data protection Regulative (GDPR), law on personal data protection (LPDP)*

1. INTRODUCTION

The rapid development of modern technologies makes our lives significantly easier, but on the other hand, it brings us problems that we have not had before, or at least we have not had them on that scale. One of the most current problems we face in this sense is information security (ISec). The field of information security, as an approach to preserving its basic properties, is generally regulated by the basic standard ISO 27001 within the ISO 27000 series (ISO 2018, 2022a, 2022b). The basic properties of information - CIA - include *Confidentiality*, that the information is available only to those who have the right to it, *Integrity*, that the information is complete and protected from unauthorized changes, and *Availability*, that the information is available when we need it, provided that we have the right to it.

The specificity of the ISO 27001 standard in relation to other management standards is reflected in the special Annex A, which, according to the latest revision of the standard from 2022 (ISO 2022a), contains 93 controls grouped into 4 categories - organizational controls (chapter 5 - 37 controls), people controls (chapter 6 - 8 controls), physical controls (chapter 7 - 14 controls) and technological controls (chapter 8 - 34 controls). In comparison with the previous revision of standard (114 controls), 11 controls are new and others are renamed, modified or merged.

^a ORCID: 0000-0002-8067-6582

Protection of personal data represents a very significant and delicate segment of the overall concept of information security. The significance arises from the fact that personal data are present in databases within information systems of various purposes - systems of state bodies (about citizens or taxpayers), banking systems (about bank clients), systems of educational institutions (about pupils, their parents, students, teaching staff), systems in healthcare institutions (about patients, staff, etc.). The delicacy is a consequence of the fact that personal data is closely related to the spheres of our lives that we do not want to share with a large number of people. At the same time, the disposal of that data opens up enormous opportunities for misuse and can have inestimable consequences for our lives.

The protection of personal data is closely related to the universal right to respect for private life, which, together with the rights to respect for family life, the right to respect for home and the right to respect for correspondence, was proclaimed by the UN Universal Declaration of Human Rights from 1948 (UN, 1948). The development of information technologies, the Internet and the information society over time led to the recognition of the need to protect personal data and it was recognized in the European Charter of Fundamental Rights, adopted in 2000 (EU, 2000), where in Art. 8 declares that "everyone has the right to protection of personal data" which must be processed in a fair way, in accordance with the purpose and with the consent of the person.

In this paper, the topic of personal data protection is considered from several points of view. Firstly, the representation of the topic in standards related to information security was reviewed. Then the key documents related to international legal regulations were discussed, i.e. General Data Protection Regulation - GDPR (EU, 2016a) and the Directive considering the application of the GDPR in the field of personal data of persons connected with the investigation of criminal offenses (EU, 2016b). Particular attention was paid to the Law on the Protection of Personal Data in the Republic of Serbia (OGRS, 2018) and the experiences and challenges of its application both at the level of the Republic of Serbia and within organizations.

2. PERSONAL DATA PROTECTION IN STANDARDS AND REGULATIONS

This chapter provides a concise overview of the ISO/IEC 27001 standard, European regulations and laws in the Republic of Serbia from the point of view of personal data protection, and then challenges and dilemmas in their application in practice are discussed.

2.1. Standard ISO/IEC 27001

The significance of personal data protection is already visible from the change in the title of the standard (ISO 2022a) which, in addition to information security includes cyber security and privacy protection. Of course, this topic is also present within controls from Annex A in several places, predominantly in organizational and people controls, Table 1:

- Explicitly, in control A.5.34, which refers to the privacy and protection of personally identifiable information (PII).
- Discussing the security related to human resources before (A.6.1 and A.6.2), during (A.6.3 and A.6.4) and after termination of engagement (A.6.5).
- Defining access rights, including authentication and authorization (A.5.17, A.5.18 and A.8.5).
- Discussing the management of incidents related to information security, including personal data breaches (A.25 to A.29).

Table 1. Controls in Annex a of ISO/IEC 27001:2022 related to personal data protection
(Source: Author)

Part	Title
A.5	Organizational controls
A.5.9	Inventory of information and other associated assets
A.5.10	Acceptable use of information and other associated assets
A.5.17	Authentication information
A.5.18	Access rights
A.5.25	Assessment and decision on information security events
A.5.26	Response to information security incidents
A.5.27	Learning from information security incidents
A.5.28	Collection of evidence
A.5.29	Information security during disruption
A.5.34	Privacy and protection of personal identifiable information (PII)
A.6	People controls
A.6.1	Screening
A.6.2	Terms and conditions of employment
A.6.3	Information security awareness, education and training
A.6.4	Disciplinary process
A.6.5	Responsibilities after termination or change of employment
A.6.8	Information security event reporting
A.8	Technological controls
A.8.5	Secure authentication

2.2. General Data Protection Regulation (GDPR)

The General Data Protection Regulation 2016/679 - GDPR, (EU, 2016a) was adopted by the European Parliament and the Council on April 27, 2016, and was published in the Official Journal of the European Union (OJEU) on May 4, 2016 and it began to be applied on May 25, 2018. The period of two years from the adoption to the application of the regulation brought many doubts about its content and the possibility of its application, which are still present today. The regulation itself has a total of 88 pages, the first 31 of which contain a preamble with 173 items, which explains the basic elements contained in the regulation. Paragraph (7) of the Preamble, which states that "natural persons should have control over their personal data", should be especially emphasized, and this can be considered an essential reason for adopting the regulation. The regulation itself is presented on the remaining 57 pages, it contains a total of 99 articles that are grouped into 11 chapters, some of which have sections. A summary of the structure of this regulation is given in Table 2 by chapter and section (where they exist). In the table in question, numbers in parentheses indicate articles of regulation that refer to individual segments.

It is important to note that alongside this regulation, directive 2016/680 (EU, 2016b) was adopted, which limits the application of the GDPR in cases related to the processing of personal data by competent authorities for the purposes of preventing, investigating, detecting and prosecuting criminal offences. The bottom line is clear - those who are engaged in criminal activities cannot invoke the protection of personal data in order to prevent investigations related to their crimes.

Table 2. Regulative 2016/679 (GDPR) structure (*Source: Author*)

Part	Title
I	General provisions (1-4)
II	Principles (5-11)
III	Rights of the data subjects (12-23)
1	<i>Transparency and modalities (12)</i>
2	<i>Information and access to personal data (13-15)</i>
3	<i>Rectification and erasure (16-20)</i>
4	<i>Right to object and automated individual decision-making (21-22)</i>
5	<i>Restrictions (23)</i>
IV	Controller and processor (24-43)
1	<i>General obligations (24-31)</i>
2	<i>Security of personal data (32-34)</i>
3	<i>Data protection impact assessment and prior consultation (35-36)</i>
4	<i>Data protection officer (37-39)</i>
5	<i>Codes of conduct and certification (40-43)</i>
V	Transfers of personal data to third countries or international organizations (44-50)
VI	Independent supervisory authorities (51-59)
1	<i>Independent status (51-54)</i>
2	<i>Competence, tasks and powers (55-59)</i>
VII	Cooperation and consistency (60-76)
1	<i>Cooperation (60-62)</i>
2	<i>Consistency (63-67)</i>
3	<i>European data protection board (68-76)</i>
VIII	Remedies, liability and penalties (77-84)
IX	Provisions relating to specific processing situations (85-91)
X	Delegated acts and implementing acts (92-93)
XI	Final provisions (94-99)

A broader overview of GDPR is given in the literature (Rakovic, 2023). It should be noted that, in accordance with the GDPR, the key participants in the processing of personal data are the "Controller" and the "Processor" - the "Controller" determines the purpose and means of personal data processing, while the "Processor" processes personal data on behalf of the controller. As per GDPR, one of the key institutions is the "consent" of the data subject to the processing of personal data, as any form of freely expressed will of the data subject by which he or she, by statement or clearly affirmative action, approves the processing of personal data relating to him or her. A key problem that arises in the processing of personal data is "Personal Data Breach", which is a breach of security that leads to the accidental or illegal destruction, loss, alteration, unauthorized disclosure or access to personal data that is transmitted, stored or processed in another way.

The processing of personal data takes place in accordance with seven principles - legality, correctness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality and accountability (EU, 2016a; Rakovic, 2023). The essence is clear - personal data can be collected and processed only in accordance with the purpose for which they are intended and in the smallest possible scope, while they must be protected from all forms of abuse. In simple words, we need to "find the right measure" in the processing of personal data, and we know how difficult this is in many areas of life.

The GDPR defines eight key rights of data subjects (EU, 2016a) - the right to be informed about the processing of their personal data, the right to receive confirmation from the controller

as to whether or not personal data have been processed, the right to correction, the right to deletion ("the right to be forgotten"), the right to ask the controller to limit processing, the right to data portability, the right to object and the right not to be the subject of decisions based solely on automatic processing, including profiling.

The GDPR foresees very high penalties for violating the security of personal data, in two levels (EU, 2016a) - an administrative fine of up to €20 million, or up to 4% of the annual income in the previous financial year, i.e. €10 million, or up to 2% of the total annual turnover income in the previous financial year, which is more unfavorable for the perpetrator! The following are examples of fining operators for non-compliance with GDPR provisions in Europe, based on data available in the literature (Diligenski, 2019):

- Google fined €50 million in France for unclear purpose of processing personal data and forwarding personal data for marketing purposes without subject's consent.
- British Airways was fined €205 million in the UK, due to the loss of data for 500,000 customers due to a website compromise.
- Facebook was fined €100 million in Belgium because the "like" button was used to profile users in order to deliver advertisements to them.
- Facebook was fined €10 million in Italy for selling user data.
- Facebook was fined €565,000 in Great Britain for allowing Cambridge Analytics to use data from a survey of 300,000 users in Donald Trump's election campaign.
- Post in Austria was fined €10 million for profiling 3 million citizens in terms of political affiliations and selling data to political parties.
- Real estate company Deutsche Wohnen in Germany was fined €14.5 million for keeping data on tenants for too long and without legal basis.

The above data refer to the year 2019, i.e. the first year after the full implementation of the GDPR. A similar trend continued after that period. For example, at the end of May 2022, the US Federal Commission fined Twitter €150 million because the company provided user information to advertisers, including phone numbers and e-mails, between May 2013 and September 2019, thereby misleading users to protect their personal data. Also, at the end of May 2023, after an investigation that has been conducted since 2020, company META (earlier Facebook) was fined €1,2 billion in Ireland due to the violation of European rules on data protection on the social network Facebook, because it transferred the personal data of users from the European Economic Area to the USA. The company was ordered to stop any transfer of personal data to the USA within 5 months.

It is interesting to analyze the relationship of the GDPR to the information security management standard ISO 27001. The analysis shows (Rakovic, 2023) that a correctly implemented information security management system according to the ISO 27001 standard **is still not sufficient** for compliance with the GDPR. Although there are many similarities between these documents, there are also significant differences. First of all, these documents differ in their character - the GDPR is a legally binding document, the non-implementation of which entails certain penalties, while the implementation of the standard is voluntary, until the organization opts for it. In addition, many institutions that exist in the GDPR do not exist within the ISO 27001 standard. This primarily refers to consent to the processing of personal data (Articles 7 and 8 GDPR), the right to erasure, i.e. "to be forgotten" (Art. 17 GDPR), the right to limit processing (Art. 18 GDPR), data portability (Art. 20 GDPR) and the right to object (Art. 21 GDPR), while the international transfer of personal data from Art. 46 of the

GDPR partially exists in the ISO 27001 standard, but primarily refers to business data. On the other hand, the standard contains details on maintaining the level of information protection, which is not present in the GDPR.

2.3. Law on personal data protection

In November 2018, the new Law on Personal Data Protection of the Republic of Serbia - LPDP (OGRS, 2018) was adopted. The constitutional basis for passing the Law in question is contained in Art. 42 of the Constitution (OGRS, 2006) which proclaims that the protection of personal data is guaranteed, that the collection, storage, processing and use of personal data are regulated by a separate law, that everyone has the right to be informed about the collected personal data and has the right to judicial protection in case of their abuse. In addition, this topic is dealt with in Art. 97 of the Constitution (OGRS, 2006) as part of the protection of freedoms and rights of citizens. The reasons for the adoption of the new LPDP lie both in internal needs to upgrade the legal system to better ensure the protection of personal data and in the context of joining the European Union, because the need to amend this Law was stated in 2016 as part of the report on Serbia's progress in the EU accession process.

The structure of the LPDP is shown in Table 3. This law essentially combined Regulation 679/2016 - GDPR (EU, 2016a) and Directive 680/2016 (EU, 2016b). A first glance at Table 3 indicates that in relation to the structure of the GDPR, sections VII "Cooperation and consistency" and X "Acts of delegation and implementation" are missing, which is a consequence of the fact that Serbia is not yet a member of the EU.

Table 3. The LPDP structure (*Source: Author*)

Part	Title	Article	GDPR
I	Basic provisions	1-4	I
II	Principles	5-20	II
III	Rights of data subjects (data subjects)	21-40	III
IV	Controller and processor	41-62	IV
V	Transfers of personal data to third countries or international organizations	63-72	V
VI	Commissioner (Independent Supervisory Authorities)	73-81	VI
VII	Remedies, liability and penalties	82-87	VIII
VIII	Special cases of processing	88-94	IX
IX	Penal provisions	95	VIII
X	Transition and final provisions	96-102	XI

The principles of the LPDP and the GDPR and data subject rights in both documents overlap to a significant extent. There are certain differences between those documents (Rakovic, 2023):

- From the point of view of applicability, the GDPR has a significant advantage over the LPDP because it contains an extensive Preamble that accompanies the regulation itself and significantly contributes to its understanding through examples, explanations and the context of its adoption. The provisions from the Preamble were not included in the LPDP, and direct application of the GDPR is not possible because we are not a member of the EU, so in practice the provisions of the LPDP remain to be implemented in the spirit of other legislation.

- Both documents contain 26 definitions of which 22 overlap and 4 differ. The LPDP defined "person whose data are processed" (in the GDPR it is "data subject", but does not appear as a separate definition), "multinational company", "authorities" and "competent authorities",

and omitted the definitions "mainly appointment of supervisory authority", "competent supervisory authority", "cross-border processing" and "relevant reasonable objection".

- The role of the supervisory body in the LPDP is taken over by the "Commissioner for Information of Public Importance and PDP".

- According to the LPDP, independent consent for the processing of personal data can be given by a person at the age of 15 (in the GDPR, 16 is recommended, but not younger than 13).

- The LPDP provides for the right to "complaint" to the Commissioner, the GDPR provides for the right to lodge an objection - appeal. Lawyers are united in their opinion that the legal effect of a complaint and an objection - appeal is not the same.

- Violations of the LPDP are subject to fines ranging from 50 thousand to 2 million RSD for 32 cases, as well as 6 cases with a fixed fine of 100 thousand RSD. It is drastically different from the GDPR because the range of fines is from €430 to €17,000. In a certain way it contradicts the view that the penal policy should act as a disincentive for offenders. The amount of the fines is far below the damage that can be caused by violating the LPDP and the profit that can be made in that way, so the violators calculate it as a "cost" of business!

It is interesting to consider the relationship between the LPDP and other regulations in the field of labor legislation in Serbia. The LPDP (OGRS, 2018) does not contain explicit provisions related to employers and employees, that is, the collection of personal data about the employee in the field of work, although in everyday work situations that require the processing of such data are frequent. Instead, Art. 91 of the LPDP (OGRS, 2018) refers to regulations in the field of work. In general, these issues are usually regulated by an employment contract or a collective agreement.

In practical application of labor legislation, it is necessary to take into account the following (Rakovic, 2023):

- That the data requested from job candidates be unambiguously related to the job position.
- That the data on the candidate who was not hired be stored for a future round of employment only if the candidate has unequivocally agreed to it.
- That medical data on the employee's state of health be limited to "remittances" confirming temporary incapacity for work, i.e. a doctor's opinion on temporary fitness for work, without details.
- That biometric data is collected only if it is necessary and if the purpose cannot be achieved in any other way (e.g. records of arrivals and departures from work).
- That data from the criminal record is collected only if it is prescribed in advance by law.
- That monitoring of employees is carried out when it is necessary (e.g. for their safety) and within the limits of "reasonably expected privacy", which is a concept developed by the European Court of Human Rights in its practice.
- That the monitoring of the employee's communication on the official phone or computer, that is, the official e-mail account, should be clearly declared in terms of the obligation to use these means of communication exclusively for business purposes, with a minimum of private communication.

- That the storage of employee data outside the Republic of Serbia, i.e. on "cloud computing" servers can only be carried out in terms of LPDP, because it has the character of presenting employee data.

2.4. Challenges and dilemmas in LPDP application

In the practical application of the LPDP, there are many dilemmas, inconsistencies and challenges, of which only the most significant are listed below (Rakovic, 2023):

- It was established a very short interval of 9 months from the entry into force of the LPDP until its implementation. In the case of the GDPR, that interval was 2 years. It was the reason why the Commissioner requested the postponement of the implementation of the LPDP from August 22, 2019. but this initiative was not accepted.

- The authorities often do not inform the Commissioner about relevant issues within his jurisdiction and often take steps without his consent. There are situations in which a large amount of data on Serbian citizens are transferred abroad, without approval of the Commissioner.

- There is still insufficient awareness among people about the importance of personal data. People usually think that they, as ordinary people, are not so important for someone to have some of their data, that they have nothing to hide, etc. In everyday life, it is possible to see that people themselves, in various forms (social networks, street surveys, public places and public transport, etc.) give their personal data to others without any need. Planned amendments to the LPDP and the adoption of the Personal Data Protection Strategy until 2030, are oriented to the introduction of education on personal data protection in primary and secondary schools.

- In the course of 2021 alone, more than 200 complaints about the violation of personal data were sent to the Commissioner (PDCS, 2021), and more than 300 inspections were carried out

- Banks or hotels often ask for an ID card, which, instead of basic identification, is read, printed and placed in some binders without any need, or kept at the reception desk during the guest's stay with the explanation that they are being asked to do so by the Ministry of Interior (MoI).

- By-laws did not resolve the issue of video surveillance in open and/or closed spaces (facial recognition technology), nor the issue of unauthorized use of photos on social networks.

- In the period from January 2015 to July 2020, the activities of the public prosecutor's office and the courts related to Art. 146 of the Criminal Code, which refers to the unauthorized collection of personal data (PDCS, 2021). The results show that out of 66 courts, in 14 there were a total of 28 cases related to that article, 4 acquittals, 2 convictions (both conditionally), and the other 22 cases were rejected as unfounded, dismissed or suspended. In the same period, the Commissioner submitted 17 criminal reports, but none of them received an epilogue, especially due to the fact that the injured parties often do not have lawyers due to their social and economic status.

- Within the unified information system (UIS) in education, there is a huge amount of data in the form of a register of students, their parents or guardians, a register of teachers, etc. as well as an electronic diary system. It was observed that the private firm that maintains that system on a commercial basis offers additional options to users in terms of access to the data of others. From the point of view of statistics, all the mentioned data should be anonymized,

i.e. that data on real persons can only be seen in special databases, which are not widely available.

- In the LPDP, art. 12, six bases are defined on which personal data can be processed while respecting the principle of legality of processing. The most flexible basis in practice is the basis of processing which is based on the legitimate interests of the operator or a third party, unless the interest of the person whose data is being processed prevails over them. The dilemma remains, where is the line where the legitimate interest ends and the private interest of the person whose data is processed begins. In general, this basis of processing requires a more careful and analytical approach, all in the context of the "reasonable expectations of the individual", as defined in paragraph (47) of the GDPR Preamble (EU, 2016a).

- At the time of the COVID-19 pandemic, healthcare came into focus because in some areas, data on the health status of people became publicly available on the websites of local governments. In this area, it was not clear who is the handler and who is the processor, and what is the legal basis for collecting, processing and disclosing that data. A drastic example is the situation when RTV Pink published a video lasting several minutes from the KCS Infectious Diseases Clinic showing several patients on ventilators whose faces were visible.

- A special segment related to the collection and processing of personal data is represented by companies - organizations that carry out these activities on the basis of the legal obligation to record the employment relationship, for the purpose of realizing the rights of employees and their family members or for the purpose of realizing the business and legitimate interest of the organization (e.g. employee references as part of the bidding and contracting process). In this sense, the principles of minimization (collecting only as much data as is necessary, no more and no less) and expediency, i.e. that for each of the data there is a clear purpose for which it is collected and processed (Reljanovic, 2020).

- In practice, there are many cases of abuse of personal data in order to discriminate against sensitive groups, e.g. women for whom, during employment, the employer requests information that is not of interest to the job, such as information on marital status and family planning, or information related to health, an extract from criminal records, etc.

3. CASE STUDY: ENTEL

The application of personal data protection is illustrated on the example of the company Energoprojekt Entel plc, Belgrade. It is the company whose activity is design, consulting and engineering in the fields of energy, water, telecommunications and environmental protection. The organization has implemented an integrated management system (IMS) with five management standards - quality, environmental protection, safety and health at work, information security and energy management, in accordance with the relevant ISO standards (EPE, 2022).

Starting from the previously stated position that a correctly implemented information security management system according to ISO 27001 is not sufficient for the full implementation of the provisions of the GDPR, i.e. the LPDP, the organization expanded its information security management system (defined by procedure EN-27P-01) with a special procedure EN-27P-02 which is dedicated to the topic of personal data protection. The subject procedure regulates: analysis (mapping) of personal data (data description, category, basis of processing, storage period, medium/location of storage, transfer to a third party, controller, processor and a more detailed description of the purpose of processing); assessment of the impact on the security of personal data; procedure in case of endangering the security of personal data; giving and revoking consent to the processing of personal data; gaining insight into the employee's personal data that is collected and processed about him and erase personal data.

The procedure has totally seven forms (EPE, 2022) - personal data register, personal data security impact assessment, personal data security impact assessment procedure, statement of consent to personal data processing, statement of revocation of consent to personal data processing, a request for insight into the personal data being processed and an order - a list for erase personal data. In addition to employees, this procedure includes the collection and processing of personal data of potential employees (who apply for a job through the organization's website) and suppliers and other business partners.

For the sake of illustration, below are listed several key decisions that the company made as part of defining the system for the protection of personal data:

- From the register of personal data, all items that could be disputed from the point of view of protection of personal data, such as the reading of an identity card, a copy of a passport as a biometric data, etc., have been omitted. For each of the items, the purpose of collection and processing is stated.
- It is defined that the official phone, computer, or official e-mail account can be used exclusively for official purposes and that the distribution of inappropriate content through these means is subject to disciplinary responsibility.
- That the data about the candidate who applied through the company's website, but was not hired, is stored for a future round of employment within a period of 12 months from the moment of application, and that it is removed after that time. The potential employee is informed about this fact in the process of applying to the site.
- Although the procedure envisages giving consent to the processing of personal data, in practice it is decided not to collect anything that would be subject to the obligation to give consent for processing. In the procedure, it is explicitly stated that the registration of children for New Year's packages, i.e. for traditional prizes for students for success achieved at school, is considered as giving consent that their names can be found on the list of persons to whom those gifts were given.
- Data on Unified Identification Number of Citizens (UINC) for employees exist within the information system, but access to that data is enabled to a small number of employees, primarily the specialists of professional services and the top management of the company.

4. CONCLUSION

In this paper, the topic related to the protection of personal data is considered from the point of view of the information security management standard ISO/IEC 27001, European regulations and laws in the Republic of Serbia. Also, some challenges, dilemmas and experiences in application of standards and regulations are discussed. It is necessary to mention that the topic is still new in our conditions and is particularly burdened by the tendency of our mentality to avoid, rather than implement, established rules. It is crucial to take measures of a preventive nature, and not to treat the consequences when problems arise. In practical application, there are many difficulties, considering that many elements are not defined by secondary legislation (use of UINC, video surveillance outdoors - traffic, parks, and indoors - shopping centers, etc.). It is very important to strengthen people's awareness of the protection of personal data, as well as their constant education in this area. The fact is that there is a lot of possibilities for improvement, but it requires time, effort and patience.

REFERENCES

- Diligenski, A. (2019). Bulletin of lawyers - practitioners, no. 9, December 2019: "Institutions in Serbia are not prepared for the new Personal Data Protection Act", www.kolega.rs. Accessed 30.05.2023.
- EPE. (2022). Energoprojekt Entel plc IMS documents
- EU (2000). Charter of Fundamental Rights of the European Union, Official Journal of European Union C 364/01, 18.12.2000.
- EU (2016a). Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, OJEU, 4.05.2016, L 119/1 to 88)
- EU (2016b). Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (OJEU, 4.05.2016, L 119/89 to 130)
- ISO (2022a). Information security, cyber security and privacy protection - Information security management systems - Requirements (ISO 27001)
- ISO (2022b). Information security, cyber security and privacy protection - Information security controls (ISO 27002)
- OGRS (2006). Constitution of the Republic of Serbia (Official Gazette of Republic of Serbia 98/2006, 115/2021 and 16/2022)
- OGRS (2018). Law on Personal data protection (Official Gazette of Republic of Serbia 87/2018, 13.11.2018)
- PDCS (2021). Privacy and protection of personal data in Serbia – Analysis of selected sectoral regulations and their application (Partners for Democratic Changes Serbia, #EU for you, Ministry for Human and Minority Rights and Social Dialogue, Belgrade, March 2021)
- Rakovic, R. (2023). Personal data protection – Framework and challenges, Belgrade: Engineering Academy of Serbia (in Serbian)
- Reljanovic, M (2020). „Protection of personal data in the employment relationship“ (Personal data protection in Serbia - Proceedings, Institute for Comparative Law, Belgrade, 2020, pp. 61-92 (in Serbian)
- UN (1948). Universal Declaration of Human Rights, UN

RESCUING FROM THE RUINS

Branko Babic¹

¹ Higher Education Technical School of Professional Studies, Skolska 1, Novi Sad, Republic of Serbia, babic@vtsns.edu.rs

Received: 25th July 2023

Accepted: 12th August 2023

Review paper

Abstract: *The process of forming specialist rescue teams from ruins started in 2009 as a part of the Emergency services sector of the Ministry of Interior of the Republic of Serbia. The teams were formed with the help of the Directorate for Civil Protection of the Ministry of the Interior and Territorial Communities of the Republic of France, whose members also trained the members of the fire-rescue units and the Gendarmerie. Specialist teams are trained so that their members who work in fire-rescue units, in addition to their regular duties, provide a quick and adequate response in case of this type of emergency. This type of organization avoids the duplication of personnel, reduces expenses, rationalizes resources, and provides well-coordinated, professional teams that act quickly and efficiently. This paper deals with the systems of saving the survivors from the ruins (height and depth).*

Key words: *rescue teams, rescue systems, ruins*

1. INTRODUCTION

Rescue from the ruins requires great courage, expertise, humanity and dedication of intervention and rescue teams, as well as the introduction of new and more modern equipment. In order to improve the work of intervention-rescue teams and their safety, it is necessary to work permanently on the professional training and improvement of rescuers, define standards and rules during the intervention and rescue services. It is also important to develop a detailed protection and rescue plans. Constant cooperation with foreign teams, through the exchange of knowledge and experience in this field, as well as the organization of joint training camps, is another way to improve the response of teams in such situations.

2. ORGANIZATION OF SERVICES AND UNITS FOR RESCUE FROM THE RUINS

At the Government of the Republic of Serbia meeting on March 5, 2009, a need to establish a service for emergency situations within the Ministry of Internal Affairs arose (Sector for Emergency Situations, n.d.). A working group was formed from representatives of the Ministry of Interior, Ministry of Defense, and other ministries of the Government, with an aim of analyzing the current situation in the field of emergency situations, reviewing and proposing necessary changes to the applicable legal norms and adopting the new ones that determine the competence and actions of certain authorities in this area (Conclusion on the adoption of the action plan for the formation of a single service for emergency situations, 2009). In the session

held on June, 26th, 2009, the Government of Republic of Serbia ratified the rulebook on revisions and amendments on the internal arrangement and systematization of workplaces in the Ministry of Internal Affairs. Based on the new systematization, the Sector for Protection and Rescue has grown into the Sector for Emergency Situations. This enables the Republic of Serbia to obtain an integrated system of protection in emergencies (Sector for Emergency Situations, n.d.). The Department for Emergencies has three organizational units in its organizational structure: 1. Directorate for Preventive Protection; 2. Administration for fire-rescue units and civil protection, and 3. Risk Management Directorate (see Figure 1). In addition to the administrations, 4 Emergency Departments were formed in Belgrade, Kragujevac, Nis and Novi Sad, along with Departments for Emergencies with the headquarters of the administrative districts.

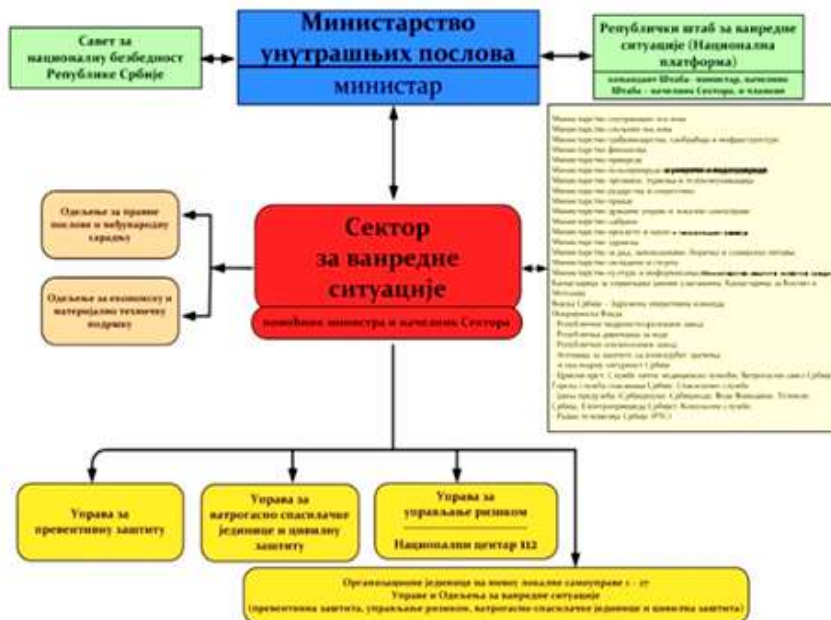


Figure 1. Organization of the emergency sector
Source: Sector for Emergency Situations, n.d.

2.1. Training of teams and formations

The training is conducted on three levels, two of which are in Republic of Serbia, and the third one is a specialist training in the centre for rescue from ruins in France. The total number of trained police officers is around 200 for levels 1, 2 and 3. The team organization was done according to INSARAG directions for USAR team forming picture 2 (Kasumacic & Salinger, 1985).

Light USAR teams (Guidelines and methodology of INSARAG, 2006) possess operational capabilities to assist with search and rescue on ground immediately after an accident, mainly coming from the affected country as well as its neighboring countries. The rescue team consists of 11 people who assigned to the Command and Group for the rescue and evacuation of the injured. The team can include canine search groups (Handbook for participants of the course for specialist teams for rescue from ruins, n.d.). In the team there can also be a medical group consisting of one doctor and one paramedic.



Figure 2. Training of members of specialist rescue teams
Source: Sector for Emergency Situations, n.d.

Medium USAR teams (Guidelines and methodology of INSARAG, 2006) possess operational capabilities for technical search and rescue operations in structural collapse incidents, capable of breaking, breaking, cutting and penetrating concrete, typically found in urban areas. International Intermediate USAR teams can travel to the affected countries and are expected to operate within 36 hours. The team consists of 46 people distributed in the following ways: the team commander and his or her deputy, the platoon command, three intervention teams, which also include pairs with canine search. The team also has a medical group composed of one doctor and one paramedic.

Heavy USAR teams (Guidelines and methodology of INSARAG, 2006) have operational capabilities for difficult and complex technical search and rescue operations at structural collapse incidents especially those involving structures reinforced with structural iron (rebar). They are intended for international assistance in the event of a sudden accident that results in the fall and collapse of multiple reinforced concrete structures, mostly located in urban areas, when the disaster response capacities of the affected country are either overburdened or the country lacks the necessary capabilities. It operates in the affected country within 48 hours. The team consists of 60 people distributed in: Command Department; Medical team; Command and Immediate Support Department; Department of Radio Communications; Media Communication Department; Technical Support Department; Logistics Department; The intervention platoon consists of three intervention departments.

Having followed the seismological map produced by the Republic Seismological Institute of Serbia, the Department for Emergency Situations formed teams according to the territorial principle (Sector for Emergency Situations, n.d.): basic teams in Belgrade, Novi Sad, Kragujevac and Nis, which are intermediate USAR teams in terms of their formation. In addition to these teams, light teams were formed in Valjevo, Bor, Uzice.

3. PERSONAL RESCUE SYSTEMS FROM THE RUINS

In cases of persons trapped on the higher floors due to the collapse of buildings and internal structures, rescue units use several techniques to access the endangered persons and safely evacuate them to the lower floors and out of the building (Handbook for participants of the course for specialist teams for rescue from ruins, n.d.) and (Kasumacic & Salinger, 1985). Rescue systems are: "HINGE", "4 POINTS"; "TYROL" (cable car); "SKATE"; "ROLLER" and "ARROW" rescue system developed by forming an arrow.

"HINGE" rescue system - the system is used for rescuing endangered persons from lower floors, and is generally limited by the length of the stretched ladders (10m) which correspond to the height of one, two and possibly 3 floors. The procedure consists of sending one group of rescuers to the floor to detect and find the victim, while the other group prepares the ladder

for descent by leaning the bottom of the ladder against the base of the wall or by tying the ladder to a fixture. After finding the victim, the first triage is performed and the victim is placed on a bed connected to the ladder, and then safely evacuated by a coordinated descent during which the group of rescuers on the ground additionally secures the bed with the help of a safety rope – figure 3.



Figure 3. Application of the "HINGE" system
Source: Sector for Emergency Situations, n.d.

The "4 POINTS" rescue system is used in evacuating lower floor victims who have to be lowered or raised in a horizontal position through an opening or hole. After completing the search of the ground and evacuating the victim to the opening where rescue is planned, one group of rescuers stays with the victim and the other goes to a higher level where they install safety ropes and connect to 4 points of the rescue trough. The technique consists in manual, uniform lifting of the vulnerable person using ropes that are tied to those 4 points of the trough. This technique is physically very demanding and depends on the physical strength of the rescuers, so it is rarely used. As this technique is mainly applied at lower levels, it is necessary to predict the leakage of explosive gases due to damage to installations during an earthquake, so it is necessary to measure the explosiveness prior rescuing and to provide rescue teams with equipment for the protection of the respiratory organs (insulation devices). Securing the terrain, searching for and setting up a place for moorings is done simultaneously with approaching the victim – picture 4.



Figure 4. "4 POINTS" rescue system
Source: Sector for Emergency Situations, n.d.

Rescue system "TIROL" (cable car) - the system is used for rescuing people from greater heights, theoretically from any floor and serves for the quick evacuation of endangered persons from high buildings. Evacuation with this technique can be carried out from the building to the ground or to the neighboring building, and even across rivers. Even though the technique allows quick evacuation, just setting up the transport system takes longer, and requires good coordination with the team on the ground – figure 5.

Rescue system "SLIDE" - the system is used to evacuate vulnerable persons from lower floors, i.e. as far as the stretcher ladder allows us (1 to 2 floors). This system is most often used because it is the simplest and fastest to set up. The injured person is placed in a rescue trough, the trough is placed on a ladder. The descent is controlled at the end of the ladder by using a safety rope on a figure "8" descender, operated by one rescuer. The injured person is placed in a bed with his or her head up, protected by a helmet and goggles – figure 6.



Figure 5. "TIROL" rescue system (cable car)
Source: Sector for Emergency Situations, n.d.



Figure 6. "SKATE" rescue system
Source: Sector for Emergency Situations, n.d.

"ROLLER" rescue system – the system is used for the evacuation of endangered persons from any floor with the help of a designed or manufactured support, i.e. anchorage ladder. The system can be hung on a ladder, a tripod, on solid pillars, on a crane, on made anchorages with the help of wooden beams, etc. This system is used when there are no other options left for pulling the victim out. It is necessary to find a solid support or place it on the spot suitable for pulling the victim out with a winch and safety ropes, at the ends of which the stretcher is fixed. This procedure allows lowering and raising – figure 7.



Figure 7. Rescue system using "ARROW" construction

Source: Sector for Emergency Situations, n.d.

"ARROW" rescue system with an improvised arrow - the construction of the arrow is done using a ladder by bringing the ladder to the place of installation. The ladder is pointed at a previously made support (anchorage). Four slings are slipped between the ladders and hooked with carabines. The so-called ropes are tied to the ends of the ropes. knot "8". We hang the ropes on all four carabines, and concurrently raise the ladder and tie the other ends of the ropes to the anchorage. When everything is secured, we climb the ladder, double check and while we are on it we can hang a roller and by using it we can pull out injured people from depths or rubbles.

4. CONCLUSION

Today, international cooperation in protection and rescue is one of the most active segments of international politics, and the exchange of experiences, experts and information is part of building a system of trust among nations and achieving stability in certain regions, and in the world as a whole. At the moment of a disaster or a major accident, a quick exchange of information about the occurrence of an accident or danger is ensured, and, if necessary, the sending of special equipment and resources or rescue teams to the affected country. The level of training of rescuers is adapted to world standards. Better equipment and constant training of members of the rescue units is a prerequisite for a safe and timely response to this type of rescue operations. Earthquakes, as one of the most severe natural disasters, puts an additional burden on rescuers in terms of a lack of operational personnel due to the fact that the team members are on a voluntary basis, without any supplements, and they are also workers of fire and rescue units, which therefore shows more formed regional teams. Until now, our country has mainly formed medium and light teams with basic sets of equipment.

All rescuers on the ground must follow the rules when acting, meaning: they have to move quietly and slowly, do not disturb the stability of the collapsed materials, always assess the durability and strength of the ground you walk on, do not move elements that support other elements (beams, furniture, etc.), do not walk near cracked walls that threaten to collapse, support such walls with some object if possible, do not use open flames or engines that can produce sparks due to possible gas leaks in the building. Personal and team protective equipment is included in the basic protection measures of the rescuer and it is used in all phases of rescuing people from the rubble. When performing a rescue operation, there are many threatening and disturbing factors, such as physical factors (noise, vibrations, poor lighting, unfavorable climatic conditions such as extreme cold and heat, high humidity, etc., biological hazards such as viruses, bacteria, fungi, parasites and the like) Additionally, constant physical effort, i.e. physical strain and non-physiological position of the body, makes it difficult for

rescuers to work. Rescuers are also exposed to very stressful situations because they are constantly under pressure and also constantly encounter severely injured people, mutilated bodies, etc., which can endanger the rescuers' mental and physical health and permanently or temporarily disable them for further work.

REFERENCES

Conclusion on the adoption of the action plan for the formation of a single service for emergency situations. (2009). Sl. Gazette of RS, no. 78/2009

Guidelines and methodology of INSARAG. (2006). Office for the Coordination of Humanitarian Affairs, July 2006.

Handbook for participants of the course for specialist teams for rescue from ruins. (n.d.). Ministry of Interior of the Republic of Serbia.

Kasumacic I. Salinger S (1985). Rescue from the ruins manual, Belgrade.

Sector for Emergency Situations Ministry of Interior the Republic of Serbia (n.d.) <http://prezentacije.mup.gov.rs/svs/HTML/delatnost.html>

COUNTERING THE THREAT OF UNMANNED AERIAL SYSTEMS TO CRITICAL INFRASTRUCTURE

Goran Maksimovic¹

¹ Security Research Center, Street Sinise Mijatovica 9, Banja Luka, Republic of Srpska, Bosnia and Herzegovina, gomax5575@yahoo.com

Received: 27th July 2023

Accepted: 22th August 2023

Original scientific paper

Abstract: *It has been observed that unmanned aerial systems (UASs), have been used in a very different way over time including both the malevolent and benevolent usage. Today, technologically developed society, demands regular provision of resources vital for own functioning whilst being heavy sensitive on its disruption. Unmanned aerial systems could pose a threat to facilities critical to the functioning of the population and the government. Having in mind their abilities, the ways they could be used malovolently is practically unlimited. Nowadays, ensuring the acceptable level of security for critical infrastructure includes the counter-UAS system as well. This paper proposes a method for building a security system for encountering the malevolent usage of UAS and allows effectiveness of the C-UAS to be assessed.*

Key words: *critical infrastructure, unmanned aerial system, detection and neutralization, C-UAS*

1. INTRODUCTION

Contemporary, technologically developed society, demands regular provision of resources vital for own functioning, not requesting unnecessary piling of supplies concurrently being heavy sensitive on its disruption. The world today has seen a number of developments as result of technological advancements. These outcomes have been demonstrated to be more trustworthy, approachable and economical in everyday lives. In addition, people now engage with one another in other ways inside their social circles. On the other side, unmanned aerial systems (UASs) are employed for both commercial and private purposes in addition to being heavily utilized in military contexts. Consequently, unmanned aerial systems could pose a threat to facilities critical to the functioning of the population and the government.

The attempt of this article is to give a comprehensive understanding of new advancements that have led to the issues surrounding unmanned aerial systems (UASs), including mostly threats, privacy concerns and other limits that are important and cannot be disregarded. A working hypothesis is that current security measures are not developed enough to adress the threat posed by UAS and need to be developed further. The major goal is to identify most of the issues related to this and to give all scholars access to a single resource that will allow them to understand the most recent trends and a thorough understanding of the subject. This paper has been organized in to five sections. The first part of the paper deals with the term of critical

infrastructure, the second is focused on determination and UAS characteristics while the section three contains options of malicious usage of the UAS. Vulnerability of the UAS is in the fourth chapter and the last one is dealing with the modes of countering the UAS threat. The overall conclusion to this work can be found on the end.

2. CRITICAL INFRASTRUCTURE AND ITS PROTECTION

Today's society requires a regular supply of resources necessary for its functioning and does not require unnecessary stockpiling, which is at the same time sensitive to supply interruptions. Because of this, the priority of protection is focused on the infrastructure that makes it possible, marked as critical. Etymologically, the adjective "critical" gives special importance to the functioning of what that adjective describes. Therefore, the term Critical Infrastructure (CI) refers to those physical resources, services and capacities of information technology, networks and infrastructure that, if disrupted or destroyed, can have serious consequences for the health, safety or economic well-being of citizens or the effective functioning of the government. Factors that make them extremely vulnerable are present in CI: complexity, interdependence and cascading effect. One of the most frequently identified shortcomings related to the protection of critical infrastructure is an incomplete understanding of the interdependence of these infrastructures.

There are two approaches to defining the term critical infrastructure: traditional, which identifies specific facilities and objects of social interest, and holistic, which focuses on the complete system, networks and their interdependence. (Maksimovic, 2022,) Although there are different approaches to its determination, basically, critical infrastructure is made up of numerous sectors. Critical infrastructure is characterized by interconnectedness so that a break in the functioning of one element of the system can lead to a break in another, i.e. to a cascade effect, causing long-term consequences for the government system, economy, security, public health and public trust. It is the mutual connection that causes the threat of one element of the critical infrastructure system to lead to a multiply increased effect of the attack and the consequences on a number of other elements of the critical infrastructure, as well as on economic stability and society as a whole.

However, complete protection does not exist and the effects of malicious activity on critical infrastructure can be reduced by risk assessment and crisis planning. Taking measures to protect critical infrastructure requires constant dialogue between the technical and security community. Protecting CI is not a new phenomenon and it is perceived from different points of view: technical, defense, economic, national security, etc. The topicality of the protection of elements of CI stems from the fact that they are connected and highly vulnerable, the increase in the number of malicious activities aimed at citizens, as well as the increasing impact of climate change. Protection represents readiness, rejection, mitigation, response or recovery from disruption or destruction of CI. These activities are aimed on preserving the performance of CI in the event of the inability to provide a defined minimum level of service and minimizing damages and shortening recovery time. Only with a systematic analysis can the object of protection, the time of onset of protection measures, definition of tactics, techniques and procedures, etc. be determined. As the nature of hazards changes rapidly and continuously, corrective measures and responses also need to be adaptive. The protection of CI is approached traditionally - by identifying specific facilities and objects and developing plans for their protection, and by a modern scientific approach (holistic) - focused on the network system and their interdependence. The measures used to achieve safety and protection of CI include personnel, technical, structural and technological measures and physical security measures. Critical infrastructure risk analysis is necessary at all levels, horizontally and vertically, using the same methods and instruments and it precedes the creation of a vulnerability assessment.

The goal of the CI protection process is to ensure the desired level of physical protection and resistance of CI elements to the effects of all threats and the recovery process in case of element function degradation. The basic standards and rules for the CI protection are included in the context of the process of building the security framework in which the CI protection system will be built. It should determine criteria for the selection of CI facilities, emphasize the importance of CI and requirements for physical protection and should be based on the specification of CI elements. There are usually three to five classes of protection and the classification is based on the measure of the impact that disabling an element of CI. Degradation levels are defined without compromising basic function, with compromising basic function and complete incapacitation. The critical infrastructure protection system creates a critical infrastructure management system. Achieving infrastructure protection, resilience and recovery include security assessment of CI elements, security measures specifications and reconstruction functions. The organization of the critical infrastructure protection system contains a number of conceptual, organizational, technological and technical measures that ensure the required level of protection of CI elements.

3. UAS DETERMINATION AND CHARACTERISTICS

3.1. Terminology and typology

The term unmanned aerial system (UAS) applies to the unmanned aerial vehicle and its associated elements, including communication links and UAS control components, which are required for the operator to maneuver efficiently in the airspace. An unmanned aerial vehicle (UAV) is an aircraft operated without direct human intervention in or on the aircraft. As noted, UAS include three key components: aircraft (UAV), a ground control system (GCS) and a bi-directional link between the UAV and the GCS (Table 1) (Ghulam et.al., 2022; Siddiqi et.al, 2022). A UAV can be controlled autonomously without a pilot and can be controlled remotely. Today, one may see the variety of several UAS being opted for commercial and domestic use mainly because they are cost effective and are controlled remotely from anywhere.

Table 1. UAS Frequencies communication link (Source: Author)

Sr.No	Bandwidth	Description	Purpose
1.	2400.000–2483.500 MHz	≤ 100mW, if the associated standard is EN 300 328 (Digital wideband data transmission equipment) ≤ 10mW, if the appropriate standard is EN 300 440 (General short-range devices).	Mostly used for short-range surveillance or short-range maneuvering missions.
2.	5470.000–5725.000 MHz	The transmitter's operational power is ≤ 1W and the power spectral density of transmission is ≤ 50mW/1 MHz. The appropriate standard is EN 301 893 (RLAN equipment).	Long stay in sky operations, used mainly for aerial photography.
3.	5725.000–5875.000 MHz	The transmitter's operative power is ≤ 25mW and the appropriate standard is EN 300 440 (General short-range devices)	Used for short-range surveillance with fast maneuvering and manipulating tasks.
4.	5030–5091 MHz	As per the International Telecommunication Union ITU, the frequency is assigned to the command and control of UAV or drones in cargo and passenger traffic and so it cannot be used for ground-based UAVs or drones.	Used in such operations where data sharing is important with ground control room (GCR)

There are various types of UAV and discussing mainly the UAV, they could be classified into four main categories as follows: rotary-wing, fixed-wing, hybrid-wing and flapping-wing. The one with a vertical take-off and landing (VTOL) feature and that can hover at a high rate are known as rotary wing. The other with the horizontal take-off and landing (HTOL) and capability to fly aggressively and glide even with heavy payloads belong to fixed-wing. Lastly, the UAVs that have both fixed and rotary wings are known as hybrid-wing. They are designed

to have features of both previously mentioned. Some of them are designed to exhibit the flying motion of an insect and here they proposed a more power-efficient wing by changing the wing stiffener pattern parametrically (de Croon et.al, 2012). An aerodynamic analysis found that this could relate to increased wing stiffness as well as indications of vortex generation during the flap cycle. The experiments reported an improved generated lift, and scaling later these flapping-wings to flapping-wing microair vehicles (FWMAVs) having the ability to perform activities in urban and interior environments. However, the successful flight of these vehicles that are replicating insect flight, has many obstacles, including their design, manufacture, control, and propulsion.

It is already shown that any UAV can be controlled remotely using a ground command and control mechanism. Therefore, these UAVs are classified based on their ability to fly over long distances without any intervention as: fully autonomous, remotely operated and remotely pilot-controlled. The military purpose UAVs have some advanced sensors, not available on commercial base, enabling it to carry additional payloads. Subdivision of UAVs could also go into five major components as follows: airframe, onboard controller, payload capability, communication system and efficient batteries. When discussing the airframe, it must consider aerodynamics, a lightweight structure and stability but the payload variation as well. Another important component is the communication system which will ensure the communication and control between a UAV and GCS. Lastly, there is a reliable power source that can help it to fly for a specific time to fulfil the task.

Table 2. UAS communication technology (Ghulam et al.,2022)

Technique	Channel Width	Band	Bit Rate	Range	Latency	Mobility Support
Wi-Fi	20 MHz	2.4 GHz to 5.2 GHz	6-54 Mbps	100 m	10 ms	Low
GPS	2 MHz	1176 to 1576 MHz	50 bps	-	10 ms	Higher
UMTS	5 MHz	700 to 2600 MHz	2 Mbps	10 Km	20-70 ms	High
5G	2.16 GHz	57 to 64 GHz	Up to 4 Gbps	50 m	-	Ultra-High
LTE	20 MHz	700 to 2690 MHz	Up to 300 Mbps	30 Km	10 ms	Very High
LTE-A	Up to 100 MHz	450 MHz to 4.99 GHz	Up to 1 Gbps	-	-	Very High

Type of Communication	Elevation in Km	Number of Satellites	Satellite Life	Handoff Frequency	Doppler	Gateway Cost	Propagation Path Loss
Geostationary Earth orbit (GEO)	Up to 36,000	3, no polar coverage	15+	NA	Low	Very expensive	Highest
Medium Earth orbit (MEO)	5000-15,000	8-20 global	10-15	Low	Medium	Expensive	High
Low Earth orbit (LEO)	500-1500	40-800 global	3-7	High	High	Cheap	Least

It could be seen in Table 2, the UAS communicates the different wireless communication methods, but at the same time, it shares that the communication will have a latency rate as well. The table also shares the channel width, band interval and most importantly, the mobility support important for UAV design. The table represents a type of communication based on satellite type of each satellite communication.

3.2. Security vulnerabilities and concerns for UAS

For UAS there is neither a standardization of policies nor the availability of wireless security which leads to several threats. Such practical validations include the crashing of UAS with many parallel requests whereas some researchers pointed out on different types of UAS vulnerability. (Siddiqi et al., 2022) Generally, most attacks are softver based, targeting the operating system or the microcontroller of the UAV. Since there are huge advancements in the technology, UAS have a high probability of experiencing such attacks, such as GPS spoofing,

signal jamming or de-authentication. The most common vulnerability types to the UAV encompass the following: malware issue, spoofing, manipulation and other common concerns, physical design and control system limitation, sensors, Wi-Fi constraints, GPS issue, firmware issue, Skyjack attacks and controller issue. (Siddiqi et al., 2022) UAS offer numerous increasing benefits with technological progress although, some of them have limited operating resources and others create diverse security, privacy and safety issues. Licensing, regularization, and over-sight and surveillance-regulating measures and regulations are a priority. As regards, network security point at the risk analysis, it is an admitted fact that the coverage is quite different as compared to any sort of wireless sensor network or any mobile ad hoc networks. The reason lays behind the resource constraints, as UAV related coverage is broader and wider than afore mentioned.

The framework that sets the rules to operate UAS in any vicinity is known as authentication, authorization and accounting (AAA), which states several privileges to the UAS controller to operate as per the mentioned administrative rights. Moreover, in case of any uncertainty or illegal activity by UAS, it is possible easily track down the operator. This is done to limit illegal surveillance, cyberattacks and privacy threats. Thus, several mechatronic engineering solutions have been presented to overcome these malicious activities. Concerning AAA, the following guidelines could be effective for UASs:

- Authorization: assigning privileges to the UAS controller to avoid any hostile takeover with administrative rights,
- Authentication: need for a rigid authentication method for UASs to avoid unauthorized access and control,
- Accounting: in case of any illegal activity by a UAS, the owner can be tracked.

Various mechanical and operational capabilities of UAS are being exploited for conducting malicious activities. Such events make UAS growth a double-edged word, the effort to make them more secure and rigid also makes them more effective for malicious activities.

Due to their portability, low cost, availability, maintainability and maneuverability UAS are a perfect choice for malicious activity. The ability to carry a wide range of attachments makes them an effective couriers for harmful items. They can carry anything, unnoticed or stealthily. Security is not the only concern for UASs. Any UAS flying over populated areas or property can malfunction and crash and that could be harmful to buildings and can injure people. It is a high probability that a UAS can be hacked or may deviate from its path due to heavy weather disturbance. Thus, there should be a reset option available which may turn the UAS to a hovering condition only and help to gain the control back. There are certain areas where UAS may face signal jammers and later, can be controlled for a cyberattack. Thus, UAS could have some sort of filter that may detect if there is any signal jammer nearby. The third safety measure is related to its design, it is necessary to avoid any harm during a crash.

3.3. Potential malicious application of UAS

UASs could be utilized generally in both purposes, malicious and beneficent. The malicious usage represents the areas and specific domains where we are witnessing an incremental increase in utilizing the UAS over the last few decades. Factors such as diligence, cost, mobility in the humans unreachable areas, payload options and risk, compel everyone to use it. Now, depending on the type of UAS, they may be used in a efficient way. Commonly, it is seen that the UAS design is dependent on the type of mission they perform in the field. Thus, categorizing them all with respect to their domains may lead to understanding their architecture in a better way.

An UAS is a universal platform that can endanger a target from different heights, with different speeds, on different flight trajectories and with different on-board equipment. It could be used to damage an object by physically hitting or transporting a device or element that will damage the target. It could be perceived as a threat, based on the totality of circumstances that their activity may encompass: cause physical harm to a person, damage property, assets, facilities or systems, interfere with the mission of a covered facility or asset, including its movement, security or protection, facilitate or constitute unlawful activity, interfere with the preparation or execution of an authorized government activity, including the authorized movement of persons, result in unauthorized surveillance or reconnaissance or result in unauthorized access to or disclosure of classified, sensitive, or otherwise lawfully protected information and many others. Many UAS incidents are caused by careless or reckless operators but an adversary can also use it in a variety of malicious ways, including mainly the following: Active - taken through physical, material means physically endangering the object of attack; Passive - logical, electromagnetic, cyber or behavioral means of endangering the object of attack.

A facility risk assessment should consider the totality of threats posed by UAS, whether these threats are caused by negligent or reckless use of UAS, criminality, terrorism or espionage. The risks associated with UAS should not be considered in isolation of other prevailing threat conditions. Considering the full range of threats will facilitate the development of a risk-based mitigation strategy that minimizes risks most pertinent to the specific object of protection. When considering the likelihood of adversary UAS usage, it is important to consider the intent, the capability of the adversary and the desired effect. The potential of UAS has been proved already and this domain covers every type of utilization in PMESII (PMESII – political, military, economic, social, intelligence and information) purpose. Equipping the UASs with appropriate equipment multiplies its applications and increases efficiency.

Today, the UAS are low cost and easily available in markets and therefore, they are easy to use for any sort of malicious activity. Their ability to carry a wide range of external payloads make them more dangerous. Moreover, their ability to reach places where human beings cannot, makes them even more lethal because they can deliver anything without coming under anyone's notice.

4. COUNTERING THE THREAT OF UNMANNED SYSTEMS

When considering the issue of countering the UAS as a threat to CI, it is mainly focused on three areas: deterrence, detection and neutralisation. Deterrence encompass a set of measures of limitation of access, education of security personnel, imposing the risk of legal sanctions when malicious use in question or conducting a form of information/media actions in order to deter possible attempt of attack. This measures encompass, having in mind issues mentioned in chapter 3.2., but are not limited to the following: UAS licencing, tracking the import of UAS, firmer law restrictions on use of UAS, especially in field of CI, designation of UAS geographic restricted/prohibited zones (UASA-R/P), increasing local community activities for building a greater cooperation which lead to greater control of the surroundings of the facility, conducting training in the field of aviation law for police, conducting training in the field of pilotage for the personnel of the physical security of the facility, masking elements of the protected facility in order to limit the amount of information obtained during an attack, building covers of installation elements to prevent damage as a result of a direct impact with a UAS or as a result of an explosion of explosives.

The current detection systems, as elements of counter-UAS (C-UAS) systems that protect facilities, operate using various features of UAV: heat, noise, the shape of the aircraft and electromagnetic radiation of various frequencies. (Yaacoub et al., 2020; Andradi et al., 2017). Detection of heat is achieved by cameras operating in the infrared band of electromagnetic

radiation The source of heat could be a lithium-polymer battery which is a usual source of electricity, rotating engines and electronic speed controller system designed to regulate the speed of rotation of the engines. Other electronic systems, including the on-board computer, do not emit large amounts of heat. It is possible to detect an object at a temperature other than that of the surrounding air space but it is possible to design the UAS in such a way that the heat emitted by it is dissipated. Methods for dissipating heat in airplanes are already known. In the case of UAS, heat dissipation is achieved by attaching sinks to heating elements of heat or by mounting heating elements in air jets. Aircraft sound is detected using microphones. However, detecting an aircraft with a microphone is relatively difficult especially because UAS may be constructed so that the propeller rotation speed is low. The rotation speed can be reduced by using larger diameter propellers resulting, little noise is emitted by the propeller. Another method may be to perform a gliding flight. Additionally, the sound may be muffled by noise emitted by the surroundings of the detection system. If the protected facility is in an inhabited area, the sound source may be public transport, cars, sounds from nearby industrial plants, and the noise of planes landing in the city. The detection efficiency of acoustic signal could be improved by using microphone arrays (Burshtein and Weinstein, 2001) but note that intensity of sound is inversely proportional to the square of the distance. The aircraft can be detected using visual methods but weather conditions are a prerequisite for detection, particularly night, fog and precipitation that could reduce the effectiveness of vision detection. There is a potential of artificial intelligence technology, that can identify the UAS on the basis of learned algorithms. The disadvantage of this system is the difficulty in teaching the system to recognise an object correctly because such approach is a long and difficult process. Additionally, if the intruder knows the rules of detection, he can build a UAS with an unusual shape. Detection is possible by detecting communication between a UAV and GCS but this is also an unreliable, inefficient method, particularly because the ability to perform a flight without communication with the GCS. Communication could also be protected by frequency hopping. Detection is possible with the radar as well, operating at different frequencies (Ochodnický et al., 2017; Quevedo et al., 2018). The construction of radar devices also uses techniques that increase the effectiveness of object detection (Maestre et al., 2019) but its effectiveness depends on distance between the UAV and the antenna.

The existing methods for neutralising UAS are not fully effective and therefore, neutralisation systems consist of devices whose operation is based on different principles. One of the neutralising methods is destroying it with laser light. The high-energy light beam may cause the UAS to fall after being hit. These systems requires good weather conditions due to the laser light is scattered on the bad water. An UAS neutralised by this method is in an uncontrolled manner because the fall could have serious consequences. This includes possible injuries of the people, fall on sensitive elements of the installations of the protected facility and inability to read the data stored on its computer. Another method of neutralisation is to catch a drone in a net. Such a net can be launched from a netgun operated on the ground by the facility security personnel, but it can also be fired from a netgun hung over another UAS as element of the facility security system. This method is effective at close range and data can be read. Another way to neutralise a UAS is an electromagnetic pulse. The range of this type of impulse can be several kilometres and is applicable on a typical UAS. Use of the UAS field by Faraday shield (Krauss, 1992) and filters placed on the electric wires in the UAV's housing, present counter C-UAS measures. Communication signal jamming between an UAV and GCS could be disturbed by the emission of an electromagnetic wave with a flat spectrum and the noise intensity uniform for all emitted frequencies. A frequently used method for neutralising a UAV is to distort the signal of the satellite positioning system (jamming) or spoof the system (spoofing) (Sahmoudi & Amin, 2009). The disturbance is that a signal is emitted from the interfering device at the frequencies at which the positioning system works using interfering

signal that is more powerful than the satellite signal and the UAS is not able to correctly determine its position. Spoofing is where a spoofing device emits a signal containing a falsified position. The UAV assesses its position on the basis of a false signal and it will fly to the place indicated by the device pointing at the wrong position instead of to the target and the attack will be ineffective. The answer to this method of defence may be navigation, which allows the position of the UAV to be determined in the absence of access to the signal of the positioning system. The low efficiency of the currently used neutralisation systems makes it necessary to look for other, new solutions. One of the recently proposed methods is to disrupt the flight of the UAV by cheating the algorithms of analysing the image recorded by the UAV's camera (Zhou et al., 2021). This method takes advantage of the weakness in which the image analysis algorithm miscalculates the UAS's distance from the obstacle as a result of camera illumination from two different light sources. By controlling the light intensity, one can make the algorithm detect an obstacle and stop the UAS's flight.

Rule-based threat detection is a new approach enabled by artificial intelligence (AI). In comparison to others, it is more reliant on technology and less on manual interaction. Signature-based detection works well for recognizing known threats, using a pre-programmed list of known threats and their indicators of compromise to operate. This could be a distinctive behavior that typically precedes a malicious network attack. A signature-based intrusion detection systems (IDS) examines network packets and compares them to a database of known indicators or attack signatures to detect any suspicious behavior. Anomaly-based IDS, on the other hand, could alert unusual behavior. Rather than looking for known indicators, anomaly-based IDS simply detects any unusual behavior to generate alarms.

To identify the false data injection attacks, one may use the rule-based approach, used to target the signal strength between the UAV and GCR. Some research papers have proposed a signature-based IDS over UAV where they addressed bioinspired cyberattacks associated with airborne networks (Yagdereli et al., 2015). Last, is the anomaly-based IDS scheme which is used against jamming attacks. The only limitation of anomaly IDS is the huge resource requirement. They are complex and difficult to identify but, both, perpetrator and method of attack, can be identified. With this, appropriate countermeasures can be implemented to avoid any future incident. In meantime, incidents among airplanes and UAS address UAS security and privacy issues. Due to an increase in cyberattacks on UASs, there is a need to introduce strict policies and standards to minimize it. With the popularity of UASs, malicious and the illegal use of UASs will likely to proliferate.

The UAS countermeasures are divided into physical and local countermeasures, which are already proposed but still can be improved. The first countermeasure for resolving security threats on UAS is classifying the attacks types, intended target and objective of the attack. There is a need to highlight the nature of the attack and some security measures against the attacks. Most of the attacks target the authentication process of a UAS which imposes need for improvement in the UAS authentication method. The wireless-based communication network suffers from numerous security issues and threats. In recent times, machine learning based intrusion detection systems have been quite successful against network threats.

The UAS detection and neutralisation systems are not sufficiently effective to detect and neutralise a UAV. Such systems should therefore be based on devices operating on different principles. The use of devices operating on different principles ensures that the system will fulfil its task in all conditions. Detection and neutralisation devices in physical protection systems are selected by assessing the probability of detecting and neutralising unwanted activity in given conditions. Detection and neutralisation systems consisting of devices operating on different principles should also be built based on the effectiveness and probability

of detecting and neutralising UAS in given conditions and in the required time. The detection and neutralisation probability assessment should take place in the same conditions as the drone detection devices are assessed. It can be performed by counting the number of detections and neutralisations of the UAV/100 flights. An additional parameter to be assessed must be the detection and neutralisation time, known as the required time. The required time is the time when a UAV is detected and neutralised early enough to activate any planned procedures in the event of an attack before to be unable to successfully end an attack. One such procedure could be to activate the neutralising devices and direct them towards the attacking UAV. The probability of UAV detection and neutralisation in given conditions and in the required time is marked as P_{dn} , with the „dn“ index being the detection and neutralisation device (DND). The total probability of the UAS being detected and neutralised by a system made of N devices is given by the formula (Łukasiewicz & Kobaszyńska – Twardowska, 2022):

$$P_{dn} = 1 - (1 - P_{dn1})(1 - P_{dn2})...(1 - P_{dnN}) \quad (1)$$

When examining detection and neutralisation devices, security personnel should remember a few principles that determine the effectiveness (and thus the probability) of detection and neutralisation. As first, the DND must be absolutely independent of each other. Independence means that these devices must have different, separate power sources, they must have different, separate protection against interruption of operation, and the DND must not influence each other in any way. Secondly, the DN equipment and the entire system must be inspected periodically. It results from the fact that each technical object may be damaged, which will result in a radical decrease in the value of P_{dn} . The control is also due to the fact that every technical object is getting old. The DN system should also be tested whenever the system operating conditions change. Lastly, the priority for the protected facility manager should be to ensure effective DN of the attacking UAV and not the cost of building the system. When designing a protection system for the protected facility, the detection devices should be selected in a way that their operation does not adversely affect the operation of other devices used in the protected facility.

5. CONCLUSION

The use of UASs has increased dramatically, marking an era of autonomous systems and vehicles. Importance of UAS increases do to their benefits for both civil and military concerns. However, with this rise in usage, a severe security concerns are also evident. The most frequent reason why these systems are chosen in any covert use is because they are accesible, available and inexpensive to obtain. There have been numerous scholar contributions that have already addressed the countermeasures, however, there are still some areas that have not been addressed and can, therefore, still be exploited for any negative purposes. In this current, technological age, these two challenges cannot be disregarded.

UAV pose a threat to facilities critical to the functioning of the population and the government. Currently built and available systems are ineffective and do not cope with the threat as desired. The situation will deteriorate when UAS swarm technology becomes popular. An additional problem is the fact that most of the facilities important to the functioning of the population, classified as critical infrastructure facilities, were designed and built at a time when UAS did not exist, and the UAS were not so widely available and used in everyday life. These objects are therefore vulnerable to a UAS attack with high probability of success. The risk of an attack by a single UAS, but also by a UAS swarm, highlights the neccecity of both of these attack methods to be taken into consideration when assessing the effectiveness of UAS DN systems. Due to the low effectiveness of C-UAS systems, and permanent building of counter counter measures, huge efforts are being made to find new, more effective methods of UAS detecting and neutralising. So, when it comes to the begining, a working hypothesis that current security

measures are not developed enough to address the threat posed by UAS and that detection and neutralisation systems are not sufficiently effective is confirmed.

Nevertheless, only an experimentally confirmed mathematical model can give a precise picture. This paper proposes a mathematical model for assessing the effectiveness of DN system, which is part of the C-UAS system. The proposed model allows, DN systems to be evaluated and identification of inefficient elements and thus the improvement of the effectiveness of the system as a whole. It is also possible to obtain a software that will support this assessment, based on this proposed mathematical model of DN system. It also makes it possible to design a three-dimensional C-UAS system in the most efficient way for a given critical infrastructure facility and thus reduce the costs of investment in C-UAS systems by eliminating the purchase of inefficient devices that do not meet the expectations of the facility's physical security personnel at the initial design stage.

As a minimum, this paper offers an examination of these pressing issues by providing a summary of the causes, as well as potential solutions although this paper presents some existing solutions and a number of recommendations.

REFERENCES

Andrasi, P., Radisic, T., Mustra, Mario and Ivosevic J. (2017). Night-time detection of UAVs using thermal infrared camera, *Transportation Research Procedia*,.

Burshtein, D. and Weinstein, E. (2001). Signal enhancement using beamforming and nonstationarity with applications to speech, *IEEE Trans. Signal Processing*,.

de Croon, G., Groen, M., De Wagter, C., Remes, B., Ruijsink, R., van Oudheusden, B. (2012). Design, aerodynamics and autonomy of the DelFly. *Bioinspir. Biomim.*

Ghulam E. Mustafa A., Saiful Azrin B. M. Zulkifli, Rana Javed Masood, Vijanth Sagayan Asirvadam and Anis, Laouti. (2022). Comprehensive Review of UAV Detection, Security, and Communication Advancements to Prevent Threats. *Drones*, Vol 6.

Krauss, J. (1992). *Electromagnetics*, 4th ed., McGraw-Hill, New York, NY.

Łukasiewicz, J., Kobaszyńska – Twardowska, A., (2022). Proposed method for building an anti-drone system for the protection of facilities important for state security. *Security and Defence Quarterly*.

Maestre, N., Mata-Moya, D., Jarabo-Amores, M., Gomez-del-Hoyo P. and Rosado-Sanz, J. (2019). Optimum beamforming to improve UAV's detection using DVB-T passive radars, *IEEE International Radar Conference (RADAR)*, Toulon, France.

Максимовић, Г., (2022). Концепт приватно-јавног партнерства и заштита критичне инфраструктуре, *Зборник Дискурс о критичној инфраструктури*, ВПТШ, Добој.

Ochodnický, J., Matousek, Z., Babjak, M. and Kurty, J. (2017). Drone detection by Ku-band battlefield radar, *International Conference on Military Technologies (ICMT)*, Toulon,

Quevedo, Á. D., Urzaiz, F. I., Menoyo, J. G. and López, A. A. (2018). Drone detection with X-band ubiquitous radar, *International Radar Symposium (IRS)*, Toulon.

Sahmoudi, Mohamed and Amin, Moenes G. 2009. Robust tracking of weak GPS signals in multipath and jamming environments, *Signal Processing*, 89(7), pp. 1320–1333,

Siddiqi, M. A., Iwendi C., Kniezova J. and Noble A. (2022). Analysis on security-related concerns of unmanned aerial vehicle: attacks, limitations, and recommendations. *Mathematical Biosciences and Engineering*, Volume 19, Issue 3.

Yaacoub, J., Noura, H., Salman, O. and Chehabm, A. (2020). Security analysis of drone's systems: Attacks, limitations, and recommendations, Internet of Things.

Yagdereli, E., Gemci, Cemal and Aktas, A. Ziya. (2015). A Study on Cyber-Security of Autonomous and Unmanned Vehicles. The Journal of Defense Modeling and Simulation.

Zhang, G., Wu, Q., Cui, M., Zhang, R. (2019). Securing UAV Communications via Joint Trajectory and Power Control. IEEE Trans. Wirel. Commun. 18.

Zhou, C., Yan, Q., Shi, Y. and Sun, L. (2021). Double Star: Long-range attack towards depth estimation based obstacle avoidance in autonomous systems, arXiv preprint. <https://arxiv.org/abs/2110.03154>.

RISK MANAGEMENT DURING THE PANDEMIC

Goran Bozic¹, Hatidza Berisa^{2a}

¹ Ministry of Defense of the Republic of Serbia, Crnotravaska 17, Belgrade, Republic of Serbia, goranbozic998@gmail.com

² University of Defence in Belgrade, National Defense School, Veljka Lukica-Kurjaka 33, Belgrade, Republic of Serbia, hatidza.berisa@mod.gov.rs

Received: 16th June 2023

Accepted: 16th August 2023

Professional paper

Abstract: *The aim and purpose of the research work "Risk management during the COVID-19 pandemic" involves presenting the basic aspects of risk management during the period of the COVID-19 pandemic caused by the severe acute respiratory syndrome of the corona virus 2 (SARS-CoV-2). In an unprecedented crisis, the first official step towards attempted management was the declaration of a public health emergency of international concern by the World Health Organization (WHO) on January 30, 2020. This pandemic has so far, according to official statistics, caused more than 676,000,000 cases and 6.88 million confirmed deaths.*

The paper aims to show that risk management is a relevant tool in the process of managing changes caused by the sudden outbreak of this pandemic and all the health, social, economic and political challenges that the whole world has faced. The work, through the theoretical and research part, should provide a basis for prevention, transformation, resilience, easier resolution and eventual prevention of future crisis pandemic situations.

Key words: *pandemic, COVID-19, risk, management, risk management*

1. INTRODUCTION

There are many risk management principles and meanings behind the term itself. Risk management is an organized way of thinking about possible risks and planning in relation to their probability and impact. The reason why it is important to understand the principles of risk management is that there will always be some risk exposure involved in the goals, whether of an individual, an organization, a country, or the entire planet. By organizing known risks into manageable parts, different strategies can be created to protect against threats or opportunities. By considering possible internal and external risks before they occur, some can be avoided entirely, some can be reduced or increased, and some can be influenced in terms of the likelihood and potential impact of something happening. Risks are a part of every human endeavor. What makes the study of risks interesting is that they have largely led to the development of humanity, from the invention of caveman tools to the most modern forms of

^a ORCID: 0000-0002-9432-5273

medical therapy. A formalized, effective risk management process ensures intelligent decision-making. This process should include defining clear goals and expectations, identifying potential risks and their likelihood of occurrence, assessing these potential risks in relation to tolerance (risk appetite) for them, determining cost-effective control measures and risk mitigation strategies for risk management, as well as educating everyone involved on how best to deal with each risk.

The purpose of the research paper "Risk management during a pandemic" involves presenting the basic aspects of risk management during a pandemic. The paper aims to confirm the hypothesis that management in risk management is a relevant tool in the process of managing changes caused by the sudden outbreak of the pandemic and all the health, social, economic and political challenges that society faces during the pandemic. The work, through the theoretical and research part, should provide a basis for prevention, transformation, resilience, easier resolution and eventual prevention of future crisis pandemic situations.

2. CONCEPTUAL DETERMINATION OF RISKS

Risk is the probability that an outcome will have a negative impact on people, systems or assets. Risk is usually expressed as a function of the combined effects of the hazard, the property or people exposed to the hazard, and the vulnerability of those exposed elements. Not all risks in the experiences of individuals are equal. Individuals tend to avoid risks that they perceive as unknown or terrifying, such as those that come with dramatically bad outcomes, such as hurricanes, pandemics, or other natural disasters. During such disasters, risks tend to mutate, change, chances are more uncertain, understanding of the unknown is less.

2.1. Types of risk

Evidently, a new and integrated academic approach is needed, in order to capture the full scope of the social experience of risk and to study the dynamic processing of risk by different participants in a pluralistic society. Such a new approach should offer a meta-perspective, which assigns each perspective its proper place and function. The understanding of risk, common management methods, risk measurements and even the definition of risk differ in different areas of practice. Some of the basic categories of risk studies in the 21st century are: political, economic, environmental risks, health, IT risks, security risks, etc. Risks can be classified according to different criteria and "all risks that affect the safety of people, property and business and represent security risks, regardless of whether they are naturally or socially determined" (Kekovic et al., 2011).

3. RISK MANAGEMENT

Risk management has perhaps never been more important than in the 21st century, as the risks facing modern organizations have become more complex, fueled by the rapid pace of globalization. New risks are constantly emerging, often linked to and generated by the now ubiquitous use of digital technology. For example, the most recent external risk that manifested itself as the COVID-19 pandemic quickly evolved into an existential threat, affecting health and safety, the way of doing business, the ability to interact, etc. Risk management is a specific process of identifying, assessing and controlling risks that come from different sources. These sources can be financial uncertainties, legal obligations, technological issues, strategic management errors, accidents and natural disasters. A successful risk management program helps an organization consider the full range of risks it faces. Risk management also examines the relationship between risks and the cascading impact they might have on the organization's strategic goals. The risk management program should be aligned with the organization's strategy. In order to connect them, risk management managers must first define the

organization's risk appetite, that is, the amount of risk it is willing to accept in order to achieve its goals.

3.1. Risk management framework and policy

The Risk Management Framework (RMF) provides a common understanding of what risk management is and introduces a common language and minimum standards and processes. Risk management frameworks can be applied to individual policy sectors or to clusters of interdependent policy sectors. Integrated risk management across sectors and levels of government recognizes that risks can intersect, overlap or lead to additional risks elsewhere, all of which would be overlooked by a single risk focus. The framework should ensure that information about risk, derived from these processes, is adequately communicated and used as a basis for decision-making and responsibility at all relevant organizational levels" (Kekovic et al. 2011). Along with the framework itself, it is also necessary that the risk management policy itself be aligned with the organization's goals. Policy states the organization's intent and guides decisions, and defines outcomes in specific and measurable terms. It is important that the risk management policy is something that can be implemented, whether it is through a strategy, or some kind of procedure or activity.

3.2. Process and principles of risk management

The concept of risk management "represents a systemic approach based on the basic assumption that it is a planned, far-sighted, structured, informative and constantly applicable activity - technique" (Karovic & Komazec, 2010). Monitoring activities should measure key performance indicators and look for key risk indicators that could trigger a change in strategy. Another essential element in the process is communication and consultation - since risk awareness is an essential part of risk management, risk managers must also develop a communication plan to communicate the organization's risk policies and procedures to employees and relevant parties.

The main principle of risk management is to provide value to the organization. In other words, risk management activities are designed to achieve the best possible outcome and reduce the volatility or uncertainty of the outcome. However, risk management operates on a broader set of principles and there have been several attempts to define these principles. Its epilogue is the ISO 31000 Standard, which includes a detailed list of proposed risk management principles.

4. PANDEMIC

The word "pandemic" comes from the Greek "pan" meaning "all" and "demos" meaning "people", and the word usually refers to a widespread epidemic of an infectious disease in an entire country or one or more continents at the same time (Honigsbaum, 2009). The definition according to the Oxford dictionary from 2001 is that a pandemic is "an epidemic that occurs worldwide or in a very wide area, crosses international borders and usually affects a large number of people" (Last, 2001), while the word epidemic itself is defined as "the occurrence in a community or region of cases of disease, specific health-related behaviors, or other health-related events that clearly exceed the normal expected duration" (Last, 2001). The World Health Organization (WHO) changed the definition of a pandemic in 2009, which defines the phases and actions in the auxiliary memoir "Descriptions of the WHO Pandemic Phases and Main Actions". All versions of this document refer to influenza, while the stages are defined by the spread of the disease.

4.1. The concept and characteristics of a pandemic

In order for the WHO to issue a level six pandemic warning, there must be continuous transmission in at least two regions at the same time. The standard WHO definition of

pandemic influenza refers to a situation in which "a new and highly pathogenic viral subtype, to which no one (or few) in the human population has immune resistance and which is easily transmitted between people, establishes a foothold in the human population of the population, whereby point is spreading rapidly throughout the world" (WHO, 2011:540-541).

4.2. The impact of the pandemic and security

The 21st century COVID-19 pandemic has reminded us of human vulnerability, but also of resourcefulness, adaptability and resilience. This health crisis had repercussions in all fields. It revealed the harmful effects and danger of misinformation, but also provided an increase in trust in science and a significant increase in scientific literacy. Science took center stage. Working around the clock from the moment news of the pandemic broke, scientists quickly sequenced the virus and solved its structure, vaccines and tests were developed, and billions of doses were produced faster than the world had ever seen before, saving many lives. The restrictions that came with the pandemic, including lockdowns and closures/restrictions on movement (lock-down), as well as strict quarantines, affected many researchers, not only in terms of their mental and physical health, but also hindered their ability to work, slowing down their careers. The fight against the pandemic has emphasized taking precautionary measures such as extensive hygiene protocol (regular hand washing, avoiding face-to-face interaction, etc.), social distancing and wearing masks, etc.

The primary focus of public authorities and the private sector was disease control. The protection of human life was the most important basis for all further steps. To this end, health systems, personnel, facilities, tests and necessary equipment had to be secured and expanded as needed. State budgets have been greatly expanded to meet the extraordinary needs. Measures introduced to limit the spread of the virus have affected personal freedom.

5. RISK MANAGEMENT DURING THE PANDEMIC

A pandemic is a problem that disrupts security at all levels. The dominance of health concerns changes the balance between production, profitability, industrial safety, occupational safety, occupational health and the environment. On the ground, the demand for pandemic management limits labor availability and makes on-site work difficult. This leads to the widespread adoption of remote work and social distancing, due to the need to protect individuals working in teams. All this has transformed and complicated the implementation of everyday security practices.

5.1. Setting the context of the problem in security, business and other environments

In the phase of setting the context of the problem, questions arise: how to ensure the resilience of the organization (in this case, the country, region, continent, at the world level...), how to prepare for an unprecedented level of uncertainty and unexpected events, how to manage security, etc. The outbreak of the COVID-19 pandemic represented a diverse emergency situation across sectors and human units. The pandemic had, above all, medical and health impacts, but also economic, security, social and psychological impacts. The measures adopted by individual governments to prevent contagion (lockdowns, travel restrictions, etc.) have had direct consequences on the world labor market, on global economic productivity, on the growth and education of younger generations, and on the mental health of individuals.

5.2. Identifying potential risks

Apart from the obvious risks to human health as a whole, various risks that the pandemic entails can be identified. According to the Methodology for preparation and content of disaster risk assessment and rescue protection plan ("Official Gazette of the RS", no. 80/2019), when

preparing risk identification, it is necessary to: determine the territory for which the risk assessment is being made; make a selection of hazards, for which the Scenario will be created.

Table 1. An example of a scenario for the potential risk of developing a strain of the "COVID-19" virus. (Source: *Methodology and contents of disaster risk assessment and protection and rescue plan, Republic of Serbia, "Official Gazette of the RS", no. 80/2019.*)

	General questions	
Danger	Hazard Name - COVID-19 "Arcturus" Danger description - deadly virus	
Appearance	Place of event - Belgrade	
Spatial dimension	Affected area - 359.96 km ²	
Intensity	Intensity of the event - Incapacitation of human resources with a tendency of daily growth	
Time	Time of appearance (time of day, month, year) - winter period (December, January, February). Cause.	
Timeline	Timeline of the development of events and what is covered - Incapacitation of human resources, burden on the health system, economic slowdown. growth etc.	
Duration	Duration - indicate direct impact on protected values - Human resources.	
Early announcement	Is the event expected -	
Preparedness	Is the population educationally prepared for the emergence of COVID-19? Do government organizations have an answer?	
Impact	Protected values	Presentation of the impact of an imagined scenario.
	Life and health of people	Total number of people affected by a process within the scenario:
	Economy/ecology	Total material damage
	Social stability	Total material damage to critical infrastructure
Generation of other hazards	Multi-risk-Danger of illness/death of people; risks of spread, burden on the health system, etc.	
Reference incidents	Were there similar events in the past and when - the outbreak of the SARS-CoV-2 pandemic, December 2019.	
Informing the public	Is there timely and accurate information?	

Table no. 1 shows the creation of the scenario. The appearance of the Corona virus, i.e. its latest strain "Arcturus", was taken as a potential danger. The content is created in order to prepare for the most likely adverse event.

5.3. Risk analysis and assessment

In the event of a pandemic, as COVID-19 has shown, it is clear that how risk is assessed and managed is important to driving policies that reduce disease transmission. Guidelines to help slow the spread of the pandemic include requiring physical distancing, quarantine, enforcing mandatory mask rules, closing businesses, testing people to see if they are infected, and contact tracing. Risk analysis and assessment is done with the help of probability assessment tools, which is shown in Table 2 below:

Table 2. Probability table. An example of a scenario for the potential risk of developing a strain of the "COVID/19" virus (Source: *Preparation methodology and content of disaster risk*

assessment and protection and rescue plan, Republic of Serbia, " Official Gazette of the RS", no. 80/2019.)

Category	Probability and frequency			
	(a) probability	(b) frequency	(c) professional judgment	Selected
1	<1%	1 event in 100 years. rarely	Negligible	
2	1-5%	1 event in 20 - 100 years.	Small	
3	6-50%	1 event in 2 to 20 years.	Medium	
4	51-98%	1 event in 1-2 years	Large	
5	>98%	1 event per year or more often	Extremely large	

The procedure for presenting the consequences is done for each of the protected values according to the scenario. The next step - showing the consequences for people's life and health, economy/ecology, social stability, etc., is done according to the same principle. After that, matrices are created for each of the protected values. If in the imagined scenario there are no consequences for any of the protected values, the risk matrix for that protected value is not displayed.

Table 3. Matrix of risks to human life and health (Source: Methodology and content of disaster risk assessment and protection and rescue plan, Republic of Serbia, " Official Gazette of the RS", no. 80/2019.)

Catastrophic	Consequences	5						Very high	
Serious		4						High	
Moderate		3						Moderate	
Small		2						Low	
Minimal		1							
				1	2	3	4	5	
			Probability						

The risk matrix is where the scenario results (consequences and probability) are combined, shown in two axes, the consequence axis and the probability axis. The matrix explains the procedure for calculating the value of risk to human life and health. The final risk value is obtained by determining the mean value of all calculated attributes.

5.4. Designing a risk management strategy, implementing and integrating the risk management process

National response strategies that have been implemented in case of outbreaks of virus pandemics are diverse. Designing a quality strategy is important in the context of understanding the real complexity and associated processes characteristic of systems in a way that facilitates the necessary multidisciplinary communication and synthesis. Developing risk management strategies allows for improved assessment of pandemic risks and countermeasures to reduce their impacts and/or likelihood of recurrence. WHO has also provided guidelines for strategic risk management planning during the COVID-19 pandemic (2022).

In order to effectively develop and implement an integrated risk management program and achieve the goals and strategies set by the organization, comprehensive research should be conducted. The benefits of integrated risk management are providing consistent and accurate

risk information, enabling organizations to meet all applicable requirements while having secure data, and helping the system deal with more than one risk.

6. CONCLUSION

Discussions about risk management in times of a pandemic are becoming more frequent on managers' agendas. The society of the 21st century, during the latest pandemic, faced a panorama of uncertainty, fear and isolation. Although it is impossible to predict all risks, especially during a pandemic, a well-planned risk management model prepares the organization to better face the challenges and uncertainties that may arise. An effective risk management model during a pandemic is essential in order to minimize the effects that organizations can bear.

Therefore, it is necessary to continuously invest in the improvement of processes and technologies, at all organizational levels, in order to define (potential) risks, as well as control points and policies to cover each of them, keeping them at the lowest levels of influence, taking into account the constant reviews and analysis of deviations, so that their work brings greater security in uncertain times. Some of the first lessons to be learned are to establish a good metric system to use for risk assessment, in order to assess the impact of risk and probability.

Good risk managers should be able to predict the next risk event likely to affect the organization. When risks evolve as quickly as they do today, managers need to know how to reorient organizational priorities. By collaborating and aligning the work performed by the various risk assurance functions, the organization can better position itself to mitigate and anticipate emerging risks.

Pandemics are becoming more frequent and severe, and pose a threat to the well-being of everyone on the planet. The COVID-19 pandemic has shown that response actions were not comprehensive or fast enough to avoid global disruption and damage.

Pandemic risk management frameworks need to be multifaceted, complex concepts that tap into many spheres of governance, including land clearing and habitat destruction, poverty, natural and cultural rights, trade, tourism, development, animal welfare, disease control, agribusiness, resource extraction and public health. All these areas must be included in the management paradigm in order to effectively deal with risk prevention and management.

It is also necessary to have a risk management plan, which provides a tool for reporting risk to senior management as well as the entire team. The results of the risk identification analyzes should be transparently available to the leaders of the organizations, in order to assist in decision-making and ensure consistent management. The best risk management practices outlined in the paper should provide key guidelines for risk-facing organizations, as well as higher-level organizational units that will need to act in the event of a pandemic.

REFERENCES

- Honigsbaum, M. (2009). Historical keyword Pandemic. *The Lancet*. Available from [https://www.thelancet.com/journals/lancet/article/PIIS0140-6736\(09\)61053-9/fulltext](https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(09)61053-9/fulltext)
Accessed: 01.08.2023.
- ISO. (2018). ISO 31000 (2nd. ed.), ISO, Switzerland, Geneva.
- Karovic, S. Komazec N. (2010). System-based risk management. Media center "Defense". Vojno delo, ISBN udk: 005.334 Belgrade.

Kekovic, Z. Savic S. Komazec N. Milosevic M. Jovanovic D. (2011). Risk assessment in the protection of persons, property and business. Center for Risk Analysis and Crisis Management. ISBN 978 86 84069 59 9, Belgrade.

Knight, H. F. (1921). Risk, Uncertainty and Profit, New York Hart, Schaffner and Marx. ISBN-10: 1614276390, ISBN-13:978-1614276395, New York.

Last, M. J. (Ed.). (2001). A dictionary of epidemiology (4th ed.). Oxford University Press, ISBN: 0-19-514168-7, New York.

Methodology and content of disaster risk assessment and protection and rescue plan (2019). Republic of Serbia, "Sl. Gazette of the RS", no. 80/2019.

WHO (2011). The classical definition of a pandemic is not elusive. Bull World Health Organ, 89(7), DOI: 10.2471/blt.11.088815.

WHO (2022). Strategic preparedness, readiness, and response plan to end the global COVID-19 emergency in 2022. Geneva, Switzerland. Licence: CC BY-NC-SA 3.0 IGO.

COMPARATIVE ANALYSIS OF NATIONAL SECURITY STRATEGIES

Bozidar Forca^{1a}

¹ Faculty of Business Studies and Law, University of UNION Nikola Tesla, Juriša Gagarina
141a Belgrade, Republic of Serbia, bozidar.forca@fbsp.edu.rs

Received: 26th June 2023

Accepted: 24th July 2023

Review paper

Abstract: *This paper is an analysis of the (national) security strategy of five countries: Spain, Poland, the Czech Republic, Lithuania and Georgia. The first four listed countries are NATO members, and Georgia aims to become one. The mentioned countries were chosen on purpose, because in the literature in our country the strategies of great powers and surrounding countries are most often analyzed. The basic research methods were historical-comparative and content analysis. The general conclusion can be as follows: The (national) security strategies of the analyzed countries are similar in approach to general security issues, but less or significantly different in terms of structure and scope of the document.*

Key words: *Strategy of (national) security; Spain; Poland, Czech Republic; Lithuania; Georgia*

1. INTRODUCTION

It is an interesting fact that the term "national security strategy" is not found in encyclopedias and dictionaries. The main reason for such a fact is the time of its (strategy) creation. In our theory, it is most often claimed that the national security strategy, as a document, was created during the time of American President Ronald Reagan (Kekovic, 2011; Kekovic & Dimitrijevic, 2017). That statement is true, but not precise. Namely, the phrase "national security strategy" actually first appeared in the USA, but not in 1987, but in the National Security Act from 1947. Namely, in Article 108 of that law, it was established that the President of the USA has the obligation to submit the National Security Strategy Report to Congress 150 days after taking office. The first such report was submitted by President Harry Truman in 1950, when that practice was stopped (Forca, 2022). Therefore, the Law on Reorganization of the Ministry of Defense (Goldwater-Nichols Act), from 1986 (Article 603), re-emphasized the stated obligation of the US President (<https://history.defense.gov/Historical-Sources/National-Security-Strategy/>). From President Ronald Reagan (1987) to Bill Clinton (end of 2000), that obligation was fulfilled almost every year. From President George Bush (the younger), i.e. from 2002, through Barack Obama, Donald Trump to Joseph Biden, the position has been taken that the national security strategy is not published every year, but that one such document is adopted during the term of the

^a ORCID: 0000-0003-4894-3772

administration of one president (Forca,2021). Thus, from 1987 to 2022, 18 documents with the general name The National Security Strategy of the USA were published in the USA. The practice of adopting a document called a (national) security strategy was accepted by the largest number of countries in the world in the 21st century.

The contents of the document called the (national) security strategy vary greatly in terms of volume (number of pages), writing style and document structure. Generally speaking, in those documents, apart from the introduction and conclusion, positions on: security (strategic) environment; security challenges, risks and threats; national values, interests and goals; security policy, that is, the mechanisms and ways of achieving national interests and goals, as well as opposing security threats and the system of (national) security. (Forca, 2021).

In this paper, the (national) security strategies of the five mentioned countries were selected for analysis. Most of the strategies are named as "national security strategy". The selection was made on purpose, that is, the countries that appear less often in domestic literature, according to the subject of this work. The general matrix of the analysis of the (national) security strategies of the seven countries mentioned includes the questions: *name of the document; editorial signatory; way (style) of writing; number of pages and document structure; challenges, risks and threats; national values, interests and goals and the national security system.*

2. NATIONAL SECURITY STRATEGY OF SPAIN

The most recent national security strategy was adopted by Spain in 2021, under the name Strategy National Security (Strategy National Security, 2021). It is an extremely voluminous document for this type of regulation, compared to other countries. Namely, the document was written on 114 pages, and the Editorial was signed by the Prime Minister of Spain, Pedro Sánchez.

The document contains the following information about the work on the strategy:

"The National Security Council was responsible for the preparation of the National Security for 2021. The creation of the Strategy is a process in which the Spanish ministries and the National Intelligence Center participated. Spanish autonomous communities and autonomous cities participated in this process, through the Sectoral Conference for National Security Issues. Furthermore, the National Security Strategy 2021 includes contributions from independent experts, individuals of renowned prestige, knowledge and experience in the field of security. The process was coordinated by the National Security Department of the Office of the Prime Minister, in the capacity of technical secretariat and permanent work. The strategy represents continuity and respects changes".

Its explicit definition is not given in the strategy, and the document itself is written in an essay style, the contents of which are structured in five main units: 1) Global security and vectors of transformation; 2) A safe and resilient Spain; 3) Risks and threats; 4) Integrated strategic planning and 5) National security system and crisis management. In addition to the five main units (parts) of the strategy, the structure of the document also includes: Summary and Introduction. The most extensive part of the document (pages 70-104) is the Integrated Strategic Planning.

A special chapter of the strategy, as we mentioned, is Risks and threats. The document explicitly lists 16 risks and threats to Spain's national security on 18 pages, which are analyzed to the extent necessary in the text. Explicitly stated risks and threats in the document are determined and elaborated in the following order:

- Strategic and regional tensions,

- Terrorism and violent radicalism,
- Epidemics and pandemics,
- Threats to critical infrastructure,
- Emergency situations and disasters,
- Espionage and foreign interference,
- Disinformation campaigns,
- Vulnerability of cyberspace,
- Vulnerability of maritime space,
- Aviation Vulnerability,
- Economic and financial instability,
- Organized and serious crime,
- Irregular migration flows,
- Energy vulnerability,
- Proliferation of weapons of mass destruction i
- Effects of climate change and environmental degradation.

In the document itself, there is no chapter on national values, interests and goals. However, in Part 2 - A Safe and Resilient Spain, when asked What is national security, three general objectives are highlighted: 1) Protection of the freedoms, rights and well-being of the population; 2) Guaranteeing the defense of Spain and its constitutional principles and values and 3) Contributing to international security, together with partners and allies, as well as commitments. Those three general goals (missions) are operationalized in the fourth unit (Integrated Strategic Planning) as three pillars of the strategy, and each pillar is elaborated through goals and sub-goals (33 activities), which is shown in Table 1.

Table 1. Pillars, goals and sub-goals (activities) *(Editing by the author)*

PILLARS	GOALS	Sub-goals
FIRST: Spain that protects lives, rights and people's freedoms and constitutional order	Deterrence and defense	1 - 3
	The fight against terrorism and violent radicalization	4 - 8
	Responding to crisis situations	9 - 12
	Counterintelligence services, fight against disinformation campaigns and action against foreign interference	13 - 16
SECOND: Spain promoting the prosperity and well-being of its citizens	Security of common global values	17 - 19
	Economic and financial stability	20
	The fight against organized and serious crime	21 - 22
	Managing of migration routes	23 - 24
	Energy security and ecological transition	25
THIRD: Spain participating in conservation international peace and security and defends its strategic interests	Strengthening multilateralism	26 - 28
	Europe strategic autonomy	29 - 30
	High profile in NATO	31 (a, b, c)
	Environmental protection, sustainable development and the fight against climate change	32 - 33

The national security system is elaborated in the last unit - National Security System and Crisis Management. The initial position in that whole states that: "The national security system includes all bodies, entities, resources, and procedures that enable the state to act in order to protect the freedom and well-being of its citizens, to guarantee the defense of Spain and its constitutional principles and values, and to together with our partners and allies contribute to international security".

At the top of the national security system is the Prime Minister, and Crisis Management consists of: the National Security Council; Connection mechanisms; Support bodies for the National Security Council (special committees) and the Department for National Security in the Office of the Prime Minister. Spain's national security system is linked to the common security of the EU and the NATO defense system. Executive parts of the system (armed forces, police, security services and others) are elaborated within pillars, goals and sub-goals.

3. NATIONAL SECURITY STRATEGY OF THE REPUBLIC OF POLAND

The most recent national security strategy of Poland was adopted on May 12, 2020, under the name National Security Strategy of the Republic of Poland. As the beginning of the document states: "The strategy was approved by the President of the Republic at the request of the Council of Ministers." By the way, the document does not contain an editorial by any of the political figures, as is the case with other foreign strategies (National Security Strategy of the Republic of Poland, 2020).

The National Security Strategy of Poland is written in essay style (smaller part) and paragraph style (larger part), on 37 pages, and has the following units: Introduction; Security environment; Values, national interests and strategic goals in the field of national security; Pillar I – Security of the state and its citizens; Pillar II – Poland in the international security system; Pillar III – Identity and national heritage; Pillar IV - Social and economic development and environmental protection and Conclusion. The most extensive part of the document is the stated pillars of the strategy.

There is no explicit definition of strategy in the document, but it says:

"The strategy offers a comprehensive vision of shaping the national security of the Republic of Poland in all its dimensions. It includes the subject-oriented aspect (the internal dimension of national security as well as the international environment – bilateral relations, regional cooperation at the global level). scale and cooperation within international organizations) and object-oriented (includes all dimensions regarding the functioning of the national security system). National interests and strategic goals in the field of national security are formulated in accordance with the national values established by the Constitution of the Republic of Poland".

There are no chapters in the strategy that are explicitly named as challenges, risks and threats, but they are discussed in the first part - Security Environment. Thus, starting from the position that challenges, risks and threats are constantly increasing, the following are listed and described as the main threats to national security:

- Explicitly, the biggest threat to security in the strategy is expressed as: the neo-imperial policy of the authorities of the Russian Federation, which is also implemented by military force,
- persistent regional and internal conflicts in the southern European neighborhood represent another risk,

- Global insecurity is also fueled by, among other things, the undermining of disarmament treaties and agreements, the proliferation of weapons of mass destruction, and the threats of terrorism and organized crime,
- the increased probability of using tactical nuclear weapons in a classic military operation, including as a means of de-escalation, is considered particularly dangerous.
- The development of solutions based on fixed and mobile broadband (5G and next generations), Internet of Things, cloud computing, quantum technologies, service automation, machine learning, nanotechnology and artificial intelligence create new development opportunities for Poland, while creating previously unknown threats, energy security, economic and financial security, health protection and climate changes.

A special part of the strategy refers to the national values and interests and strategic goals of Poland in the sphere of security.

A) *Values*: independence and sovereignty of the state, security of its citizens, human and civil liberties and rights; dignity, justice, national identity and heritage, democratic rule of law, solidarity, international order based on the principles of international law and environmental protection.

B) *National interests*: 1. Preservation of independence, territorial integrity, sovereignty and security of the state and its citizens. 2. The formation of an international order, based on solidarity and respect for international law, which guarantees the security and safe development of Poland. 3. Strengthening national identity and preservation of national heritage. 4. Ensuring conditions for sustainable and balanced social and economic development and environmental protection.

"The mentioned national interests form the pillars of the national security of the Republic of Poland." Their implementation is ensured through the achievement of strategic goals arising from them, which requires the planning and implementation of specific tasks and the possession and use of appropriate forces, means and capabilities". Each of the mentioned pillars (national interests of Poland) is operationalized and developed into 2-6 strategic goals (Table 2), which is the most extensive part of the strategy.

Table 2. National interests (pillars) and strategic goals of Poland in the security sphere (*Editing by the author*)

PILLARS	STRATEGIC GOALS
Security of the state and citizens	Managing national security State resilience and common civil defense Polish Armed Forces Cyber security Information space
Poland in the international security system	The North Atlantic Treaty Organization and the European Union Bilateral, regional and global cooperation.
Identity and national heritage	National identity of the Republic of Poland Creating a positive image of Poland
Social and economic development and environmental protection	Protection of health and family Migration policy Economic security Energy security Protection of the natural environment Scientific and technological potential

In the strategy, there is no separate unit in which the national security system of Poland is determined, but in Pillar 1 (Security of the state and citizens), in the part that talks about the Integral management of national security, there is a clause: "For the implementation of the above measures, the Law on the management of national security". Implicitly, the national security system of Poland consists of a civilian and a military part, which are an integral part of NATO and EU security and defense.

4. NATIONAL SECURITY STRATEGY OF THE REPUBLIC OF LITHUANIA

The National Security Strategy of the Republic of Lithuania was adopted in 2017. (The National Security Strategy of the Republic of Lithuania, 2017). The document is written in paragraphs on 20 pages (22 paragraphs), and is structured into the following parts: 1. General provisions, 2. Basic assumptions of the national security policy, 3. National security interests of the Republic of Lithuania, 4. Threats, dangers and risk factors, 5. Priorities and objectives of the national security policy and 6. Final provisions. The strategy does not have an editorial signed by a political figure, as is the case in most strategies of foreign countries.

The General Provisions for the Strategy contain the following definition:

"The National Security Strategy (hereinafter: the Strategy) represents a set of provisions for defining the development of a secure state. The strategy defines the vital and primary interests of national security, key risk factors, dangers and threats that represent these interests, sets priorities and long-term and medium-term goals for the development of the national security system and foreign, defense and internal policies. The strategy is based on the Constitution of the Republic of Lithuania, the Law of the Republic of Lithuania on the Basics of National Security, the agreements of the North Atlantic Treaty Organization (hereinafter: "NATO") and the European Union (hereinafter: "EU"), as well as on the strategic goals and guidelines specified in NATO and EU documents".

A separate part of the document is called Threats, Dangers and Risk Factors, with a general introductory statement: "In the dynamic, complex and unpredictable security environment of the Republic of Lithuania, external and internal, military and non-military threats, dangers and risk factors are interconnected." Taking into account the changed security environment, conventional military threats to the Republic of Lithuania or any other country in the region are no longer just theoretical, as military and non-military (diplomatic, informational, cyber, economic, energy, financial, legal) measures against the national security of the Republic of Lithuania they can be used at the same time trying to influence the most vulnerable areas in the country". In accordance with the above, 15 threats, dangers and risk factors have been identified in the strategy:

- conventional military threats caused by the capacity and willingness of the Russian Federation to use military force to achieve its goals,
- covert military and intelligence threats used by foreign countries that can be used in an attempt to negatively influence the political system of the Republic of Lithuania,
- threats to the unity of the Euro-Atlantic community,
- regional and global instability - conflicts arising in countries outside NATO and the EU,
- terrorism, extremism and radicalism,
- information threats (military and non-state),
- cyber threats,

- economic and energy dependence, economic vulnerability,
- the development of unsafe nuclear energy projects near the borders of the Republic of Lithuania,
- social and regional exclusion and poverty,
- demographic crisis,
- corruption,
- organized crime,
- emergency situations on the international and national level i
- crisis of values.

A special chapter of the document is called National Security Interests of the Republic of Lithuania. Those interests are determined as: 1) vital and 2) primary.

A) Vital interests

- 1) sovereignty, territorial integrity, democratic constitutional order;
- 2) civil society, respect for human and civil rights and freedoms and their protection;
- 3) peace and prosperity in the country.

B) Primary interests:

- 1) sustainability and unity of NATO and the EU, security, solidarity, democracy and well-being of all countries of the Euro-Atlantic community;
- 2) security, stability, spread of democratic and European values in all states located in the eastern neighborhood of the Republic of Lithuania;
- 3) sustainability of state development: economic, energy, environmental, informational, cyber, social security.

The most extensive chapter of the strategy is the National Security Policy, which is elaborated in the section called Priorities and Objectives of the National Security Policy. In the strategy, 18 priorities were determined, which were operationalized into 77 goals, designated as long-term and medium-term (Table 3).

Table 3. Priorities and objectives of national security policy (*Editing by the author*)

PRIORITIES	NUMBER OF LONG-TERM AND MEDIUM-TERM GOALS
Strengthening the capacity of national defense	7
Strengthening NATO collective defense	5
Strengthening NATO crisis management and partnership	3
Strengthening EU unity and solidarity	6
Strengthening bilateral and multilateral relations	7
Active participation in strengthening international security and stability	6
Development of a system for identification, assessment and warning of threats, dangers and risks for national security	1
Strengthening intelligence capability	1
Strengthening national capabilities for crisis prevention and management	1

PRIORITIES	NUMBER OF LONG-TERM AND MEDIUM-TERM GOALS
Strengthening civil protection	1
Strengthening common security	4
Strengthening national capabilities to fight terrorism, violent extremism and radicalization.	1
Ensuring information security and security of the Lithuanian political system	7
Strengthening the preparedness of the society for the defense of the state, strengthening the civil society and the cultural and national identity of the country	7
Strengthening economic and energy security	8
Strengthening cyber security	5
Strengthening social security, improving the demographic situation	4
Ensuring environmental protection	3

In the strategy, there is no separate chapter on the national security system of Lithuania, but it is emphasized that the security of Lithuania is part of the security of NATO and the EU, of which the country is a member.

5. SECURITY STRATEGY OF THE CZECH REPUBLIC

In 2015, the Czech Republic adopted the document Security Strategy of the Czech Republic (Security Strategy of the Czech Republic, 2015). The document is written in paragraph style (104 paragraphs), on 27 pages, and the Introduction was signed by the then Prime Minister Bohuslav Sobotka. Apart from the paragraphs, the document specifically emphasizes two parts: 1) Security threats and 2) The security system of the Czech Republic. Apart from the Introduction, the document is divided into the following parts: 1. Introduction, 2. Principles of the national security policy of the Czech Republic; 3. Security interests of the Czech Republic; 4. Security environment and 5. Strategy for the promotion of security interests of the Czech Republic. The last chapter is the most extensive.

In the Introduction to the document, the strategy is defined as follows:

"The Security Strategy of the Czech Republic is the Czech Republic's basic security policy document that serves as a reference framework for related strategies and policy concepts. It is a government act drawn up in consultation with the Cabinet of the President of the Republic and the Parliament of the Czech Republic with the aim of seeking non-partisan approaches to security issues. The security community of the Czech Republic, including representatives of the government and the non-governmental sector, was also involved in the development of this strategy".

As stated, 11 security threats are specifically emphasized (beyond paragraphs) in the strategy, namely:

- Weakening of the cooperative security mechanism, as well as political and international legal obligations in the field of security,
- Instability and regional conflicts in and around the Euro-Atlantic area,
- Terrorism,
- Proliferation of weapons of mass destruction and means of their delivery,
- Cyber attacks,

- Negative aspects of international migration,
- Extremism and the rise of inter-ethnic and social tensions,
- Organized crime, i.e. serious economic and financial crime, corruption, human trafficking and drug-related crime,
- Threats to the functioning of critical infrastructure,
- Interruptions in delivery of strategic raw materials or energy i
- Disasters of natural and anthropogenic origin and other emergency situations.

Considering the time of creation, the strategy points out (in the section: Security environment) that the threat in the form of aggression is slightly more likely. A special chapter of the strategy is named Security Interests of the Czech Republic. Those interests are classified in the document as: 1) Vital, 2) Strategic and 3) Other important interests (Table 4).

Table 4. Vital, strategic and other important interests (*Editing by the author*)

VITAL INTERESTS	STRATEGIC INTERESTS	OTHER IMPORTANT INTERESTS
<p>Vital interests include: preservation of the sovereignty of the Czech Republic, territorial integrity and political independence and preservation of all constituent elements democratic rule of law, including the guarantee and protection of fundamental human rights and freedom of the population</p>	<p>security and stability, especially in the Euro-Atlantic area,</p> <ul style="list-style-type: none"> • preventing and managing local and regional conflicts and mitigating their effects, • maintaining the UN's global stabilizing role and increasing its efficiency, • strengthening the cohesion and efficiency of NATO and the EU and maintaining the functioning and credible transatlantic relationship, • strengthening of NATO-EU strategic partnership, including strengthening cooperation in the complementary development of defense and security capabilities, • the development of the role of the OSCE in preventing armed conflicts, in democratization and in building mutual trust and security, • a functional and transparent conventional arms control regime in Europe, • supporting and developing regional cooperation, • supporting international stability through cooperation with partner countries, • supporting democracy, basic freedoms and principles of the rule of law, • preservation of internal security and protection of the population, • preserving the economic security of the Czech Republic and strengthening the competitiveness of the economy, 	<ul style="list-style-type: none"> • reduction of crime, with an emphasis on economic crime, organized crime, information on crime and the fight against corruption, • strengthening the counter-intelligence and defense intelligence services of the Czech Republic, • fostering a tolerant civil society, combating extremism and its causes, • make government institutions and the judiciary more efficient and professional; for this purpose, improving the cooperation of state administration bodies with citizens and with legal and natural persons engaged in economic activities • development of citizens' associations and non-governmental organizations dealing with security, • improvement of public awareness and active involvement of the general public in the provision of security services, • scientific and technological development, with emphasis on new technologies and high added value of innovation,

VITAL INTERESTS	STRATEGIC INTERESTS	OTHER IMPORTANT INTERESTS
	<ul style="list-style-type: none"> • preserving the energy, raw material and food security of the Czech Republic and the appropriate level of strategic reserves, • preservation of cyber security and defense of the Czech Republic, • prevention and suppression of security threats affecting the security of the Czech Republic and her allies. 	<ul style="list-style-type: none"> • development of technical and technological possibilities for processing and transmission confidential and sensitive information, with an emphasis on information protection and accessibility, • environmental Protection.

As well as security threats, the document pays special attention to determining the security system. In this sense, the strategy for the security system of the Czech Republic states:

"To protect its security interests, the Czech Republic establishes and develops a comprehensive, hierarchical security system that combines the political (domestic and foreign), military, internal security, population protection, economic, financial, legislative, legal and social levels. The system is based on laws that define the competences of individual components (legislative, executive and judicial authorities, local governments, legal and natural persons), their mutual relations and their relations with entities outside the security system, as well as their duties.

The security system of the Czech Republic provides an institutional framework/tool for creating and implementing security policy. The main function of the security system of the Czech Republic is to manage and coordinate the work of individual components responsible for the protection of the security interests of the Czech Republic. The security of the Czech Republic is not only the task of structures explicitly designed for this purpose; authorities and local administrations, legal and natural persons, but everyone contributes their part in accordance with the law.

The structure of the security system consists of: the President of the Republic, the Parliament of the Czech Republic, the Government, the National Security Council and its working bodies, central government bodies, regional and municipal offices, the armed forces, the armed security corps, intelligence services and rescue and emergency services. The overall responsibility for the security of the state, as well as for the management and operational capability of the overall security of the system belongs to the Government, as the supreme authority of the executive power".

6. CONCEPT OF NATIONAL SECURITY OF GEORGIA

The National Security Concept of Georgia is written in essay style on 28 pages, and is structured into the following parts: 1) Introduction, 2) Security Environment, 3) National Values of Georgia, 4) National Interests of Georgia, 5) Threats , risks and challenges to the national security of Georgia and 6) National security policy priorities. The most extensive part is the last chapter, which makes up 50% of the document (National Security Concept of Georgia, 2018).

The concept begins with a statement from the Constitution of Georgia: "It is the strong will of the citizens of Georgia to establish a democratic order, economic freedom, social rule of law, to ensure universal human rights and freedoms and to strengthen state independence and peaceful coexistence with other nations..." In the Introduction of the document for the concept, it is stated: "The concept of national security of Georgia is a basic document that explains the

fundamental national values and national interests, the vision of the safe development of the nation, threats, risks and challenges, and determines the main directions of the national security policy". The concept does not have an editorial document signed by a political figure, representative of the government.

Threats, challenges and risks are a separate chapter of the document, in which they are identified as follows: Occupation of Georgian territories by the Russian Federation and acts of terrorism organized by the Russian Federation from the occupied territories; The risk of renewed military aggression by Russia; Violation of the rights of internally displaced persons and refugees from the occupied territories; Conflicts in the Caucasus; International terrorism and transnational organized crime; Economic and social challenges; Energy challenges; Cyber threats; Environmental challenges; Demographic challenges; Challenges of civic integration and Destruction or damage to monuments of cultural heritage.

National values (6) and national interests (14) of Georgia are two separate chapters of the document, but in this paper they will be presented together for easier comparison. (Table 5).

Table 5. National values and national interests of Georgia (*Editing by the author*)

NATIONAL VALUES	NATIONAL INTERESTS
Preservation of sovereignty and territorial integrity Freedom Democracy and the rule of law Security Prosperity Peace	Ensuring sovereignty and territorial integrity Developing state institutions and strengthening democracy Development of an effective national security system Strengthening national unity and civil harmony European and Euro-Atlantic integration Ensuring stable long-term economic growth Ensuring energy security Ensuring regional stability Strengthening the transit role of Georgia Ensuring the environmental security of Georgia and the region Taking care of civic integration and preservation of national and cultural distinctiveness Strengthening cyber security Demographic security Relations with the diaspora

There is no separate chapter on the national security system of Georgia in the document. Data on that system are found in the third stated national interest - Development of an effective national security system, where only one position is stated: "Georgia aims to create a security system that guarantees the further development of Georgian statehood and the safety of its citizens".

7. CONCLUSION

The paper analyzes the security strategies of five countries, of which four are NATO members, one aims to become a member of the Alliance. In accordance with the comparison criteria matrix, it can be concluded:

A) *name of the document*: In 3 cases the document was named as National Security Strategy, in one (Lithuania) as National Security Concept, and in one (Czech Republic) as Security Strategy;

B) *signatory of the editorial*: Three documents do not have an editorial, and two do. The editorial was signed by the presidents of government (Spain and the Czech Republic);

C) *way (style) of writing*; Three documents were written in essays, two in paragraphs;

D) *number of pages and structure of the document*; The number of sides is very different and varies from 20 (Lithuania), 27 (Czech Republic), 28 (Georgia), 37 (Poland), to 114 (Spain). The structure of the document is very different;

E) *challenges, risks and threats*; Challenges, risks and threats are a mandatory part of the document, whether they are explicitly (a separate chapter) or implicitly (within the document). Their number is different: 9 (Poland), 11 (Czech Republic), 12 (Georgia), 15 (Lithuania) to 16 (Spain);

F) *national values, interests and goals*; There is a very different approach to determining national values, interests and goals, in terms of their name, operationalization and number;

G) *national security system*. Data on the national security system are stated explicitly and implicitly. States that give implicit access to the national security system, pass a special law for it.

The results of the analyzed security strategies show the different approach of individual countries and can be an inspiration for our approach to security issues.

REFERENCES

Forca B. (2021). Sistemi bezbednosti, Fakultet za poslovne studije i pravo, Beograd.

Forca B. (2022). Teorijski i uporedni aspekt analize strategije nacionalne bezbednosti Republike Srbije, Monografija, Fakultet za poslovne studije i pravo, Beograd.

Internet: <https://history.defense.gov/Historical-Sources/National-Security-Strategy/>
Accessed:06.05.2023.

Kekovic Z. (2011). Sistemi bezbednosti, Fakultet bezbednosti, Beograd

Kekovic Z. Dimitrijevic I. (2017). Sistemi bezbednosti sa sistemom nacionalne bezbednosti Republike Srbije, Fakultet bezbednosti, Beograd.

National Security Act (1947). Internet: <https://www.dni.gov/index.php/ic-legal-reference-book/nationalsecurity-act-of-1947> Accessed: 06.05.2023.

National Security Concept of Georgia (2018). Internet: <https://newstrategycenter.ro/documents/>. Accessed: 15.05.2023.

National Security Strategy of the Republic of Poland (2020). Internet: https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_and_2020.pdf, Accessed: 15.05.2023.

National Security Strategy of the Republic of Lithuania (2017). Internet: <https://www.newstrategycenter.ro/wp-content/uploads/2019/07/2017-nacsaugstrategijaen.pdf>, Accessed: 15.05.2023.

Security Strategy of the Czech Republic (2015). Internet: https://www.army.cz/images/id_8001_9000/8503/15_02_Security_Strategy_2015.pdf, Accessed: 15.05.2023.

Strategy National Security (2021). Internet: <https://newstrategycenter.ro/documents/>, Accessed: 15.05.2023.

TOOLS TO REDUCE VULNERABILITY FROM HYBRID THREATS

Tatjana Georjinova¹

¹ University „Sv. Kliment Ohridski” Bitola, Faculty of Security Skopje, Republic of North Macedonia, tatjana.georjinova@uklo.edu.mk

Received: 3th July 2023

Accepted: 4th August 2023

Professional paper

Abstract: *Building national resilience is the primary responsibility of member states because countering hybrid threats relates to national security and defense. However, today many member states face common threats that can be effectively addressed at the level of the European Union. In the paper, the author analyzes the need – to combine European and national instruments in building the resistance of the member states to hybrid threats and in preventing, reacting and recovering from the crisis. In the final part, the author analyzes the instruments whose application is aimed at creating the ability to detect and reduce vulnerability from hybrid threats in order to increase the ability to respond. In the concluding observations, the author gives recommendations in the direction of how each national country can efficiently and effectively deal with hybrid threats (Establishing cooperation with EU and NATO institutions, intended to deal with hybrid threats; the complexity of hybrid threats requires the full involvement of all institutional stakeholders in the national security system; Promotion of cooperation and exchange of information at the national and international level; Building high-quality and trained key personnel, as well as maintaining the basic principles of national security and resilience of society through constant basic training).*

Key words: *hybrid threats, building resilience, hybrid threats vulnerability*

1. INTRODUCTION

In recent years, the security environment of the European Union has been changing dramatically. Many of the current challenges to peace, security and prosperity stem from instability in the EU's immediate neighborhood and the changing forms of threats. They have an impact on the internal and external security of the EU. Today, many member states face common threats that can be more effectively addressed at the level of the European Union. The European Union can be used as a platform to strengthen national efforts and through its regulatory capacity, establish common benchmarks that can help raise the level of protection and resilience across the EU. The EU can therefore play an important role in improving our collective situational awareness, in building Member States' resilience to hybrid threats and in crisis prevention, response and recovery.

2. HYBRID THREATS AS A CONCEPT

The term hybrid threat refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. Such actions are coordinated and synchronized and deliberately target democratic states' and institutions' vulnerabilities. Activities can take place, for example, in the political, economic, military, civil or information domains. They are conducted using a wide range of means and designed to remain below the threshold of detection and attribution. Hybrid action is characterized by ambiguity as hybrid actors blur the usual borders of international politics and operate in the interfaces between external and internal, legal and illegal, and peace and war. The ambiguity is created by combining conventional and unconventional means – disinformation and interference in political debate or elections, critical infrastructure disturbances or attacks, cyber operations, different forms of criminal activities and, finally, an asymmetric use of military means and warfare (Hybrid CoE, 2022).

By using the aforementioned unconventional and conventional means in concert, hybrid actors conceal their action. The use of different intermediaries – supports the achievement of these goals. A hybrid action is cost-effective because it turns the vulnerabilities of the target into a direct strength for the hybrid actor. This makes hybrid action more difficult to prevent or respond to. The ongoing transition in international power structures provides a fertile environment for hybrid action. The intensifying conflict of values between the West and authoritarian states erodes international norms and institutions and makes open Western societies targets of comprehensive hybrid action. A conflict of values that extends to the domestic sphere of Western societies increases polarization and disunity within and among Western actors, making them more vulnerable to external interference. Recent developments in modern technology and an increasingly complex information environment provide powerful instruments for hybrid actors if not properly countered by the Western community.

Accordingly, Hybrid CoE characterizes hybrid threats as: (Hybrid CoE, 2022), (Steingartner & Galinec, 2021).

- Coordinated and synchronized action that deliberately targets democratic states' and institutions' systemic vulnerabilities through a wide range of means.
- Activities that exploit the thresholds of detection and attribution, as well as the different interfaces (war-peace, internal-external security, local-state, and national-international).
- Activities aimed at influencing different forms of decision-making at the local (regional), state, or institutional level, and designed to further and/or fulfill the agent's strategic goals while undermining and/or hurting the target (Available at <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/>)

3. A COMMON FRAMEWORK FOR DEALING WITH HYBRID THREATS

During 2015, the European Commission and the High Representative adopted a Common Framework for Countering Hybrid Threats and Fostering the Resilience of the European Union, its Member States and Partner Countries, while increasing cooperation with NATO to counter these threats (See more: http://europa.eu/rapid/press-release_MEMO-16-1250_en.htm - https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_1250).

The Joint Framework offers a comprehensive approach to improve the common response to the challenges posed by hybrid threats to Member States, citizens and the collective security of Europe. It brings together all relevant actors, policies and instruments to both counter and mitigate the impact of hybrid threats in a more coordinated manner. In particular, it builds on the European Agenda on Security adopted by the Commission in April 2015, as well as on

sectorial strategies such as EU Cyber Security Strategy, the Energy Security Strategy and the European Union Maritime Security Strategy. Together with the upcoming European Union Global Strategy for foreign and security policy and the Defense Action Plan, and ongoing work on capacity building in support of security and development (CBSD) in third countries, the Joint Framework is part of the strategy of the Commission and the High Representative to increase the EU's capacity as a security provider.

The Joint Framework brings together existing policies and proposes twenty-two operational Actions aimed at:

- *raising awareness* by establishing dedicated mechanisms for the exchange of information between Member States and by coordinating EU actions to deliver strategic communication;
- *building resilience* by addressing potential strategic and critical sectors such as cyber security, critical infrastructures (Energy, Transport, Space), protection of the financial system from illicit use, protection of public health, and supporting efforts to counter violent extremism and radicalization;
- *preventing, responding to crisis and recovering* by defining effective procedures to follow, but also by examining the feasibility of applying the Solidarity Clause (Article 222 TFEU) and the mutual defense clause (Art. 42(7) TEU), in case a wide-ranging and serious hybrid attack occurs;
- stepping up the cooperation and coordination between the EU and NATO as well as other partner organizations, in common efforts to counter hybrid threats, while respecting the principles of inclusiveness and autonomy of each organization's decision making process.

The Framework is designed to provide a robust foundation to support Member States in countering hybrid threats collectively, supported by a wide range of EU instruments and initiatives.

The Joint Framework outlines proposals to build resilience in areas such as cybersecurity, critical infrastructure, protecting the financial system from illicit use and efforts to counter violent extremism and radicalisation. In each of these areas, the implementation of agreed strategies by the EU and the Member States, as well as Member States' full implementation of existing legislation is a key first step, while some more concrete proposals have been put forward to further reinforce these efforts. The Joint Framework addresses the challenges raised by the specificities of threats of a hybrid nature, but EU action is not limited to countering hybrid threats. EU internal policies already aim at increased resilience and prevention, and at a rapid and effective response to crisis.

4. A BASIS FOR BUILDING RESILIENCE AND DEALING WITH HYBRID THREATS IN THE REPUBLIC OF NORTH MACEDONIA

In the Republic of North Macedonia, a Strategy for building resilience and dealing with hybrid threats has been adopted (According to <https://www.mod.gov.mk/storage/2021/12/Nacionalna-Strategija-za-gradene-otpornost-i-spravuvane-so-hibridni-zakani-april-2021.pdf> accessed on 15.05.2023).

The goal of this strategy is to create national resilience, as well as efficiently and effectively deal with hybrid threats. To achieve this goal, the Strategy is aimed at creating the ability to detect and reduce vulnerability from hybrid threats while seeking to increase the ability to respond, in accordance with the framework established by NATO and the EU. The activities of the state will be divided into six areas of operational activities.

During 2016, the faces new pressures such as population growth, urbanization, land and ecosystems' degradation, the lack of natural resources, fragility of states and complex conflicts. Hence the need to build resilience. Resilience is the ability of an individual, a household, a community, a country or a region to withstand, cope, adapt, and quickly recover from stresses and shocks such as violence, conflict, drought and other natural disasters without compromising long-term development (Available at https://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/EU_building_resilience_en.pdf).

Resilience can be built at various levels. The notion of the resilience of NATO member states through maintaining and developing their individual and collective defense capacity is rooted in the Alliance's 1949 Founding Treaty. This is, in particular, established in Article 3 where the internal dimension of resilience is implicitly defined in terms of capabilities and the capacity for collective defense is operationalized through NATO's defense planning and capability development process. NATO defines resilience as "a society's ability to resist and recover from such shocks" as natural disaster, failure of critical infrastructure, or a hybrid or armed attack (According to "Resilience and Article 3", NATO, 2021).

This definition touches on two features of resilience: First, resilience concerns the ability to absorb and recover from a state of crisis (Ben Caves et al., 2021).

Second, resilient actors must be able to respond to a range of potential shocks, both expected and unexpected. This relates to the ability to survive; as one widely adopted definition of resilience puts it, an actor must be able "to maintain its core purpose ... in the face of dramatically changed circumstances" (Andrew Zolli and Ann Marie Healy, 2012).

Hence, each member state has an obligation to Build Resilience in accordance with Article 3 of the North Atlantic Treaty – the obligation to collectively and individually develop capacities to respond to any form of threat or crisis that aims to threaten society and democratic values and to destabilize the functioning of state institutions.

Resilience and Article 3 – Civil preparedness is a central pillar of Allied resilience and contributes to the achievement of the Alliance's collective defense.

The principle of durability in Article 3 of the founding agreement of the Alliance: "In order to more effectively achieve the goals of this Agreement, the parties, separately and jointly, through continuous and effective self-help and mutual assistance, to maintain and develop their individual and collective capacity to resist armed attacks".

Article 3 helps give NATO the means to fulfill its core tasks, especially the realization of collective defense. The individual commitment of each Ally to maintain and strengthen its resilience reduces the vulnerability of NATO as a whole. Resilience is first and foremost a national responsibility. NATO agreed on seven basic requirements for national resilience against which allies can measure their level of preparedness; these requirements reflect the essential functions of continuity of government, essential services to the population and civilian support of the military. In 2016, the Warsaw Summit was held where the allied leaders decided to strengthen NATO's resilience. These seven basic requirements determine the following contents:

- Continuity of government and critical government services ensured: for example the ability to make decisions, communicate and implement them in crisis conditions;
- Flexible energy supply: back-up plans and electricity networks, internal and cross-border;

- The ability to effectively deal with the uncontrolled movement of people and to deconflict these movements from NATO military deployments;
- Ability to deal with mass casualties: ensuring that civilian health systems can cope and that sufficient medical supplies are stocked and secured;
- Resilient civil communications systems: ensuring that telecommunications and cyber networks function even in crisis conditions with sufficient backup capacity. This requirement was updated in November 2019 by NATO Defense Ministers, who highlighted the need for reliable communications systems including 5 G, robust options for restoring these systems, priority access to national authorities in times of crisis and through assessments of all risks to communication systems;
- Resilient transport systems: ensuring that NATO forces can move quickly across Alliance territory and that civil services can rely on transport networks, even in crisis situations.

5. INSTRUMENTS FOR DETECTING AND DEALING WITH HYBRID THREATS

The Strategy for Building Resilience and Dealing with Hybrid Threats from 2021, identifies instruments whose application is aimed at creating the ability to detect and reduce vulnerability to hybrid threats (see more about this <https://www.mod.gov.mk/storage/2021/12/Nacionalna-Strategija-za-gradene-otpornost-i-spravuvane-so-hibridni-zakani-april-2021.pdf>).

The application of these instruments seeks to increase the ability to respond in accordance with the framework established by NATO and the European Union. The activities of the state are divided into six areas of operational activities – political instruments, economic instruments, military forces, civilian instruments, information instruments and the need to protect critical infrastructure.

Political instruments – A key effect to be achieved in the sphere of politics is the continuity of power. For that purpose, a system for early warning and notification of possible threats will be built, as well as identification and training of key personnel. An effective crisis management system will also be provided to support government activities in times of crisis with spare capacities for independent operation for a period of one month, as well as secure communication links. The following activities are undertaken in this area: achieving protection of the election process from hybrid threats, hostile cyber-activities, information operations conducted by other state and non-state entities and financing of political parties, politicians and non-governmental organizations by external factors.

Economic instruments – The second area of operational activities is the consideration of the economy and favorable business climate. The effect to be achieved in this area is the establishment of a functional mechanism for inclusion of risks related to foreign direct investment. Creating conditions for the development of the domestic economy should additionally achieve significant trade and energy independence. Creating conditions for a digital economy will enable domestic companies to compete in world markets, especially in the European Union market, as well as create new jobs and their rapid transformation of market changes. An essential activity in this area is the fight against corruption.

Military forces – The third area of operational activities is: the security-defense sector, that is the military and security forces and institutions. In this area, it is crucial to build the capability of the military security forces and the capacity to manage and support in times of crisis, in order to increase the resilience of society to deal with hybrid threats. The fact that the use of conventional armed forces is minimized in the case of a hybrid threat indicates the need for continuous improvement of the defense and security mechanisms. In this regard, it is necessary

to achieve a high ability to deal with multiple simultaneous attacks on civilian and military targets, the ability to establish an effective mechanism for security of food and water resources, dealing with uncontrolled movement of significant numbers of people and dealing with incidents that have resulted with many casualties. In addition, the intelligence entities of the Republic of North Macedonia should maintain continuous mutual cooperation and cooperation with the intelligence institutions of the EU and NATO, responsible for the assessment of hybrid threats.

Civil instruments – The fourth area of operational activity is civil society. In fact, hybrid warfare is designed to achieve social divisions and provoke riots to overthrow the government, primarily through disinformation and psychological operations. Therefore, it is necessary to create the ability for critical awareness and media literacy among the citizens of the Republic of North Macedonia. A high level of inter-ethnic and inter-religious tolerance should also be achieved in the civil sector.

Information instruments – The fifth area of operational activities is the information sector. A key effect needed to deal with hybrid threats in this sector is the creation of the ability to detect misinformation and psychological operations, as well as the ability to deal with Internet "trolls" and use artificial intelligence in the process of spreading false news and misinformation. One of the effects to be achieved is the creation of a permanent and effective system for strategic communication, directly led by the Government of the Republic of North Macedonia and in cooperation with other relevant state institutions. In addition, a situation should be reached in which the public service broadcaster will carry out planned activities to deal with false news and misinformation. At the same time, the state will support the citizens' associations that are active in dealing with misinformation.

The sixth area of operational activities is the protection of critical infrastructure of the Republic of North Macedonia. The first effect to be achieved is the adoption of a legal solution that will determine the critical infrastructure, as well as the adoption of regulations for its protection. In this context, the regulations of the European Union and NATO will be a framework for the future activities of the Republic of North Macedonia in determining and providing critical infrastructure.

Another essential element in dealing with hybrid threats related to critical infrastructure is the diversification of energy sources and suppliers. To achieve this, it is necessary to have infrastructure that will enable a high level of energy independence of the Republic of North Macedonia from individual external energy suppliers. The same concept of avoiding addiction should be used in relation to infrastructure based on new technologies such as mobile, internet and satellite communication. The Republic of North Macedonia, in terms of determining the critical infrastructure and planning its security, will take into account the technological development and the impact of new high technologies.

The Republic of North Macedonia should create a secure traffic infrastructure, reliable energy sources and transport, telecommunications network, stable health and social system, independent media and economic-financial system, as a basic part of critical infrastructure, because the complexity of hybrid threats requires full involvement of all institutional actors in the national security system.

6. CONCLUSION

Building resilience is a long-term process that needs to be context-specific and embedded in national development policies and planning. In order to realize the protection of national interests and create national resilience of society, each country needs to build an effective concept for dealing with a series of challenges as well as defense against cyber and hybrid

threats – each country should be able to adapt to the unpredictable, complex and a changing security environment.

In building national resilience, the use of following three methods: detection, rejection and response.

Detection of the threat – As a way to deal with hybrid threats, detection implies having the ability to obtain relevant and timely information about the attacker's potential intentions from all domains and media. Due to the complex nature of hybrid threats, stakeholders in all fields need to develop early detection methods (in Macedonia this role is played by the National Coordinating Council of the Intelligence – Security Community). The method to be used to successfully detect threats includes identifying critical national vulnerabilities, associating the vulnerabilities with possible scenarios and assumptions about an attacker's goals and capabilities and determining indicators to link the vulnerabilities and measures to be taken to address the hybrids threats.

Rejection of the threat - The ability to repel a threat is a method aimed at building resilience, building the capacity to withstand stress and the ability to overcome the damage caused by threats, as well as the ability to retaliate against an attacker. Resilience is needed, above all. In areas targeted for hybrid attack, such as politics, economics, the defense and security sectors, the information sector, civil society and critical infrastructure.

Response to the threat – Responding to hybrid threats means having an effective decision-making process at the strategic level. In Macedonia, the responsible body for giving directions, making conclusions and proposing measures to respond to hybrid threats, as a threat to national security, is the Council for Coordination of the Intelligence-Security Community (See more about this <https://www.mod.gov.mk/storage/2021/12/Nacionalna-Strategija-za-gradenotpornost-i-spravuvane-so-hibridni-zakani-april-2021.pdf>).

A key factor in this process is having a credible assessment of the situation and determining the level of threat tolerance, the overcoming of which would indicate that the country is subject to attack using hybrid methods. It is therefore necessary to realize effective inter-institutional communication and cooperation, coordination of intelligence services and a fast and efficient political decision-making process. Availability of credible and timely information on hybrid threats against the Republic of North Macedonia will assist the decision-making process, as well as the process of activating the assistance mechanisms of the European Union and NATO's collective defense system. Various mechanisms can be used in response to a hybrid attack, such as economic sanctions against countries, companies and individuals, expulsion of diplomats, intelligence operations and other activities to neutralize hybrid threats. However, it is essential that the response be modeled in a way that does not cause the threat to escalate, but will force the attacker to discontinue hybrid activities due to their ineffectiveness, as the damage they will suffer from such activities will outweigh the potential benefits.

In order for each national country to efficiently and effectively deal with hybrid threats, the author makes the following recommendations: Establishing cooperation with EU and NATO institutions, intended to deal with hybrid threats; the complexity of hybrid threats requires the full involvement of all institutional stakeholders in the national security system; Promotion of cooperation and exchange of information at the national and international level; Building high-quality and trained key personnel, as well as maintaining the basic principles of national security and resilience of society through constant basic training.

REFERENCES

Zolli A., Healy A. M. (2012). Resilience: Why Things Bounce Back (New York, Simon & Schuster), 7. Italics in original.

Caves B et al. (2021). "Enhancing Defence's Contribution to Societal Resilience in the UK", RAND Corporation.

Hybrid CoE. (2022). Hybrid threats as a concept. Available at: <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/> (accessed on 10.06.2023);

Resilience and Article 3. (2021). NATO

Steingartner, W., Galinec, D. (2021). Cyber threats and cyber deception in hybrid warfare. Acta Polytechnica Hungarica, 18 (3).

http://europa.eu/rapid/press-release_MEMO-16-1250_en.htm

https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_1250

https://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/EU_building_resilience_en.pdf

<https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/> (accessed on 10.06.2023);

<https://www.mod.gov.mk/storage/2021/12/Nacionalna-Strategija-za-gradene-otpornost-i-spravuvane-so-hibridni-zakani-april-2021.pdf> accessed on 15.05.2023).

LEGAL REGULATION AND CONTROL OF THE SECURITY SYSTEM OF THE REPUBLIC OF SERBIA

Zorana Ivetic^{1a}, Jovanka Tosic^{2b}

¹ Educons University, Faculty of Security Studies, Vojvode Putnika 87, Sremska Kamenica, Republic of Serbia, zorana.ivetic@educons.edu.rs

² Educons University, Faculty of Security Studies, Vojvode Putnika 87, Sremska Kamenica, Republic of Serbia, jovanka.tosic@educons.edu.rs

Received: 4th August 2023

Accepted: 16th August 2023

Professional paper

Abstract: *The state's security system includes a set of primary and secondary, permanent and temporary, internal and external, short-term and long-term goals. Goals are interrelated and have their place in the hierarchy of priorities. Each system is part of a larger system, and each country forms several large systems, subsystems and microsystems. The security system of the Republic of Serbia is regulated by law and the National Security Strategy as a set of functionally interconnected state bodies that are responsible for the security of the Republic of Serbia and its citizens. The national security system consists of subject-wise and hierarchically different contents. Control is an important aspect of the security system because it measures, evaluates and improves the efficiency and effectiveness of the work of state authorities responsible for the security of the Republic of Serbia and its citizens. The paper analyzes the normative-legal framework of the security system of the Republic of Serbia, as well as the control of the security system, with an emphasis on internal and external control.*

Key words: *security system, Republic of Serbia, legal arrangement, security*

1. INTRODUCTION

Legal regulation of the security area is of special interest to states, because states use law to pursue their vital interests. The security system is regulated by the Constitution, laws and the National Security Strategy, a set of functionally interconnected state bodies that are responsible for the security of the Republic of Serbia and its citizens. The security system consists of subject-wise and hierarchically different contents, i.e. subsystems.

The elements of the security system in the broadest sense are: activities, measures, tasks, subjects and forces. Subjects and forces make up the "brain and skeleton" of the system, and they contribute to the achievement of the system's goals with their competence, scope, equipment and method of action. Activities are the most important element, because they are

^a ORCID: 0000-0003-0629-8189

^b ORCID: 0000-0001-6025-3542

used to realize the function of the system, i.e. securing such a state in the state and society by which most or all threats to its vital values are eliminated or neutralized. System measures are the actions (procedures) that the state undertakes to move its security and defense forces from a normal to an elevated state, in order to respond appropriately to danger. The tasks of the security system are the actions and procedures used to achieve the security tasks (Djukic, 2017).

2. SECURITY SYSTEM

When defining the concept of security, it starts from the position that security is the basic attribute of every state and that it is related to its protective function. As a function in a certain society, the security system can be organized differently. The state's security system includes a set of primary and secondary, permanent and temporary, internal and external, short-term and long-term goals. Goals are interrelated and have their place in the hierarchy of priorities.

According to the Lexicon of Foreign Words and Expressions, a system can be defined as an organized whole composed of various things or knowledge (Vujaklija, 1980). In the organizational sense, a system is a set of different elements, which function as a harmonious whole, in order to achieve a certain goal. According to the Military Lexicon, security in relation to its essence and real meaning can be defined as a state, organization and function (Military lexicon, 1981). As a state, it represents the protection of some good, value, asset, society, and as a function, it is an inseparable attribute of the state, regardless of the character of the arrangement.

The security system can be defined as a form of organization and functioning of society in the implementation of measures and activities on a preventive and repressive plan, which are undertaken to preserve the sovereignty and integrity of the state, its constitutional order, rights and freedoms of citizens, as well as all other social and international values from all forms and carriers of threats, regardless of the place and time of execution (Stajic, 2021). It is a very complex system and is organized through a hierarchical structure, i.e. subsystems and microsystems. Subsystems perform one activity, as part of a general activity. Microsystems connect several smaller activities and function in a narrower space. The specificity of the security system is reflected in the organization of subsystems as a system, because each subsystem has special strengths, means, rules and work methods.

3. NORMATIVE-LEGAL FRAMEWORK OF THE SECURITY SYSTEM OF THE REPUBLIC OF SERBIADESIGN AND RESEARCH PROBLEMS

States strive to legally regulate all forms of social relations, including the area of security. The legal regulation of the area of security is of special interest to states, because states use the law to realize their vital interests and other interests, due to which they ensure by law the limitation or suppression of those activities that threaten their interests (Stajic, 2021). Regulation of the security sector based on the principles of the rule of law is particularly important, because the actors of the security sector can directly influence the political trends in society, the life and property of citizens through their actions. Therefore, it is of inestimable importance that the actions of these actors are in line with firm and pre-defined legal rules (Hadzic & Stojanovic-Gajic, 2012).

The Constitution of the Republic of Serbia is the highest legal act from which all other legal regulations, as well as all political documents, originate and are harmonized (Constitution of the Republic of Serbia, 2021). The area of human and minority rights and freedoms, economic regulation, jurisdiction of the Constitutional Court, territorial regulation, constitutionality and legality are regulated by the Constitution. In accordance with the Constitution, the security

system protects the basic values of the social community. The role of the security system derives from Article 97 of the Constitution of the Republic of Serbia.

The Constitution regulates the security system, directly or indirectly, as a whole or through individual subsystems. It also regulates the competences and mutual relationship of the highest authorities in all aspects of the functioning of the state. In accordance with the principles of separation of powers, the Constitution defines the security competences of the National Assembly, the President of the Republic and the Government, which form the governing and commanding part of the national security system, to which all state administration bodies from the executive branch of government are subordinate, including those that make up the state sector security (Hadzic & Milosavljevic, 2013). In addition to the Constitution, Constitutional laws legally regulate parts of the security system of the Republic of Serbia.

The state strategy is a general and integral programmatic standpoint for the preservation and achievement of the highest national values and interests, with the engagement of the state's mental, spiritual and material potentials for its protection and successful development, through the achievement of defined goals in peace and war. It is a general idea about the real and/or virtual direction of the political, economic and military power of the state in order to protect and achieve the highest national interests through the realization of special and individual strategies (Kovac, 2003).

The National Security Strategy is the highest strategic document, the implementation of which protects the national values and interests of the Republic of Serbia from challenges, risks and security threats in all areas of social life (National Security Strategy of the Republic of Serbia, 2019). Represents the starting point for the preparation of other strategic and doctrinal documents, public policy documents and normative-legal acts in all areas of social life and the functioning of state bodies and institutions, in order to preserve and protect the security of citizens, society and the state. It sets the framework within which the Government can and should act when adopting other general acts and documents, as well as the key parameters according to which the legal and by-law rules in the security system should be shaped. The main starting points of the National Security Strategy are: preservation of sovereignty and territorial integrity, military neutrality, care for the Serbian people outside the borders of the Republic of Serbia, European integration and an effective rule of law. The Strategy analyzes the strategic environment of the Republic of Serbia, assesses the challenges, risks and threats to the security of the Republic of Serbia, formulates national interests and goals, determines the national security policy, then the structure and principles of the functioning of the national security system, as well as the manner of its implementation.

The Defense Strategy of the Republic of Serbia defines defense as a function of the state that ensures the protection and realization of defense interests. Defense interests are an expression of the highest values and general needs of the citizens and the Republic of Serbia for the construction and preservation of security and stability as essential prerequisites for the free and democratic development of society (Defense Strategy of the Republic of Serbia, 2019). By protecting its defense interests, the Republic of Serbia simultaneously creates the necessary preconditions for the protection of all other national interests, as well as for active participation in the protection of common values with other countries. The defense strategy of the Republic of Serbia is based on the Constitution of the Republic of Serbia and the National Security Strategy of the Republic of Serbia. It is a basic strategic document that directs the development of normative, doctrinal and organizational solutions for the defense system, defense planning and financing, and the deployment of defense resources of the Republic of Serbia.

The national security system consists of state institutions and bodies that manage, plan, organize, coordinate and implement prescribed measures and activities in the security system.

This institutional part of the security structure of the security system consists of the management and executive part. The management part is part of the state apparatus that makes laws and decisions of strategic importance for the security system.

The governing part of the security system of the Republic of Serbia consists of: the National Assembly of the Republic of Serbia, the President of the Republic of Serbia and the Government of the Republic of Serbia. The responsibilities of this part of the security system are regulated by the Constitution in accordance with the principle of separation of powers. The National Assembly, the President and the Government form the governing and commanding part of the national security system, to which all state administration bodies from the executive branch of government are subordinate, including those who make up the state security sector (Hadzic & Milosavljevic, 2013). Bodies that deal with systemic activities within the security system, i.e. the activities by which the security system is constituted, changed and directed, form the management part of the system, while the authorities and organizations that carry out operational tasks for the execution of the security policy, guidelines and tasks established by the management bodies, form the executive part of the system (Dragisic, 2011).

The National Assembly is assigned the exercise of constitutional and legislative power. The National Assembly is therefore authorized to enact and amend the Constitution, decide on changing the borders of the Republic of Serbia, call a republican referendum, ratify international treaties, decide on war and peace, declare war and state of emergency, supervise the work of the security services, pass laws and other general acts, adopts the defense strategy, budget and final account and grants amnesty for criminal offences (Constitution of the Republic of Serbia, 2021). In addition, it establishes permanent working bodies (committees) and temporary working bodies. Two permanent committees are important for the security system: the Committee for Defense and Internal Affairs and the Committee for the Control of Security Services.

The Committee for Defense and Internal Affairs is considering: the draft law and other general act in the field of military, labor and material obligations, mobilization, state of emergency and war, status and other issues of professional members of the Serbian Armed Forces, military education, international cooperation in the field of defense and military cooperation, maintenance of public order and peace, gatherings of citizens, road traffic safety, state border security and control of border crossing and movement and stay in the border zone, stay of foreigners, traffic and transportation of weapons, ammunition, explosives and other dangerous materials from the scope of the ministry responsible for internal affairs, fire protection, citizenship, unique identity number of citizens, residence and residence of citizens, identity cards, travel documents, international aid and other forms of international cooperation in the field of internal affairs, including readmission, illegal migration and asylum.

In its work, the Committee for the Control of Security Services supervises the constitutionality and legality of the work of the security services, supervises the compliance of the work of the security services with the National Security Strategy, the Defense Strategy and the security and intelligence policy of the Republic of Serbia, respect for political, ideological and interest neutrality in the work of the security services, the legality of implementation special procedures and measures for the secret collection of data, proposal of budget funds needed for the work of the security services and supervises the legality of spending budget and other funds for work, considers and adopts reports on the work of the security services, draft laws, other regulations and general acts within the competence of the services, initiates initiatives and submits proposals for laws within the jurisdiction of the services, considers proposals, petitions and petitions from citizens sent to the National Assembly in connection with the work of the security services and proposes measures to solve them and informs the applicant thereof,

determines the facts about established illegalities or irregularities in the work of the security services and their members and makes conclusions about it and reports to the National Assembly about its conclusions and proposals (Rules of Procedure of the National Assembly of the Republic of Serbia, Article 66).

According to the Constitution, the President of the Republic of Serbia commands the Serbian Armed Forces and appoints, promotes and dismisses the officers of the Serbian Armed Forces (Constitution of the Republic of Serbia, 2021). In accordance with the Law on the Basics of Organizing the Security Services, the President of the Republic presides over the National Security Council (Law on the Basics of the Organization of Security Services, 2012). The President convenes meetings of the Council for National Security, determines the draft agenda for the Council session, signs conclusions and other acts of the Council for National Security, invites leaders of other state bodies and institutions to Council meetings. The Law on Defense determines the responsibilities of the President of the Republic in the defense system. The President of the Republic submits to the National Assembly a proposal to declare a state of war and emergency, approves the draft of basic development planning documents, approves the Doctrine of the Serbian Armed Forces, approves the draft of other basic strategic-doctrinal documents, orders the implementation of the Defense Plan of the Republic of Serbia, approves the Mobilization Plan of the Serbian Armed Forces, orders the implementation of preparedness measures, general and partial mobilization, adopts the Plan for the use of the Serbian Armed Forces and orders its use, adopts guidelines for building the operational and functional capacity of the Serbian Armed Forces, appoints and dismisses the Chief of the General Staff of the Serbian Armed Forces (Defence Act, 2018). In addition, the president forms the military cabinet for matters under his jurisdiction related to defense.

The Government of the Republic of Serbia is the holder of executive power in the Republic of Serbia. In the security system, the Government manages ministries and institutions in the domain of national security in accordance with the Constitution and laws. In addition, the Government proposes and implements the national security policy, directs and controls the functioning of the national security system, provides material and financial resources for the needs of national security and manages the activities of state bodies, organizations, institutions, natural and legal persons in the area of national security (Kekovic, 2009). In accordance with the Constitution and the law, the Government of the Republic of Serbia ensures the implementation of international treaties and agreements in the field of national security.

The National Security Council determines the basis of the national security policy and defines the basic measures and activities for the preservation and improvement of national security and the protection of vital national interests (Kekovic & Dimitrijevic, 2017). The National Security Council considers issues in the areas of: defense, internal affairs and security services, their mutual cooperation, as well as cooperation with other state bodies. In addition, the National Security Council monitors and coordinates the work of elements of the national security system (Kekovic & Dimitrijevic, 2017). The sessions of the National Security Council are chaired by the President of the Republic. The other members of the session are: the Prime Minister, the Minister of Internal Affairs, the Chief of the General Staff of the Serbian Armed Forces, the directors of the Security and Information Agency, the Military Intelligence Agency and the Military Security Agency. The Office of the National Security Council ensures the professional and technical working conditions of the National Security Council.

The Office of the Council for National Security and Protection of Secret Data is an expert service of the Government of the Republic of Serbia. The Office of the Council for National Security and Protection of Secret Data performs the following tasks: acts on requests for issuing certificates and permits; ensures the implementation of standards and regulations in the

field of protection of secret data; takes care of the execution of international obligations and concluded international agreements between the Republic of Serbia and other countries, or international authorities and organizations in the field of protection of secret data and cooperates with the appropriate authorities of foreign countries and international organizations; creates and manages the Central Register of Foreign Secret Data; suggests a security questionnaire form; proposes a form of recommendation, certificate and permit; keeps records of issued certificates, or permits, as well as records of refusal to issue certificates, or permission; organizes training of secret data users in accordance with standards and regulations; proposes to the Government a plan for the protection of secret data for extraordinary and emergency cases; revokes data confidentiality in accordance with the provisions of the Law on Data Confidentiality; after the termination of public authorities that do not have a legal successor, performs tasks related to the protection of secret data; cooperates with public authorities in the implementation of the Law on Data Secrecy within its jurisdiction; performs other tasks provided for by the Data Confidentiality Act (Data Privacy Act, 2009). Work with data is regulated in several system regulations. Among the most important laws are: Law on Free Access to Information of Public Importance, Law on Protection of Personal Data, Law on Confidentiality of Data, etc.

Subsystems of the security system of the Republic of Serbia are also important for the security system, which include: intelligence and security system, police system, defense system, protection and rescue system and other subsystems of importance for the security system.

4. CONTROL OF THE SECURITY SYSTEM OF THE REPUBLIC OF SERBIA

Control is a term that denotes a set of competences, powers, procedures, forms, methods and means established by the constitution and law, the use of which directly checks, measures, determines, evaluates and improves the efficiency and effectiveness of the work of state authorities, which are responsible for the security of Serbia and its citizens (Hadzic, 2012). The goal of the control is insight into the regularity and efficiency of the performance of the security function. This implies: determination of facts regarding the observance of legal competences, duties, authorizations, limitations and responsibilities in the implementation of activities, jobs and security measures (Mijalkovic, 2018). The result of the control is the determination of irregularities in the implementation of the security function, the identification and sanctioning of those responsible for omissions and errors, as well as the reprimanding of those who improved security and identified new security needs and deficiencies.

Considering the nature of control, security system control mechanisms include: political control, administrative control, control by independent state institutions and control by the public (Mijalkovic, 2018). All the mentioned types of control can be divided into internal and external control mechanisms. These two types of control differ from each other according to the origin of the control holder. Competence for internal control is assigned by law to a separate body, body or unit that organizationally belongs to a given apparatus of state power or the competent ministry, or administrative authority, while external control is performed by a state authority and/or body, which is outside the composition of the security actor that is subject to control (Hadzic, 2012).

External control of the security system is based on the principle of publicity of the work of state bodies and a critical evaluation of their actions. This type of control is manifested through: national security councils, independent and independent bodies, media, citizens, non-governmental organizations, etc.

The executive branch has a key role in shaping and conducting the security policy. Also, the executive branch has a significant role in controlling the provision of security through bodies in charge of coordination, such as the National Security Council. The National Security Council determines basic national security policies and defines basic measures and activities for the preservation and improvement of national security and the protection of vital interests (Law on the Basics of Organizing the Security Services of the Republic of Serbia, 2012).

Parliamentary control includes all mechanisms, i.e. procedures, means and methods available to the parliament in the process of regular and extraordinary control and supervision of the security system. Parliament with its permanent and temporary bodies and mechanisms responsible for the security system: reviews, changes and adopts the budget for the security system, examines the activities in the security system in the implementation of the planned security policy, examines the activities in the security system, represents a forum for reviewing the security policy and implementing measures and activities in the security system between political parties as representatives of citizens (Kekovic & Dimitrijevic, 2017).

Judicial authorities have a role in the supervision of the security sector by ensuring that the entities of the security system adhere to the internal and international legal framework in their work. Judicial control should be carried out by regularly established courts, in accordance with the law and independent of political influence. Courts do not have the authority to directly control the security system, but it is a form of secondary or intermediate controls. Although it is not considered an integral part of the process of control and supervision of the security system, the Constitutional Court can indirectly control the security system within its jurisdiction. According to the Constitution of the Republic of Serbia, the Constitutional Court is an autonomous and independent state body that protects constitutionality and legality and human and minority rights and freedom, and in this way the Constitutional Court exercises control over general acts that regulate the operation of the security system (Constitution of the Republic of Serbia, 2021).

Control by independent and independent state bodies in the Republic of Serbia can be divided into two groups: bodies established by the Constitution and bodies and bodies established by law. The first group includes the Protector of Citizens and the State Audit Institution. The laws established autonomous and independent state bodies such as: Anti-corruption Agency, Commissioner for Information of Public Importance and Protection of Personal Data, Commission for the Protection of Rights in Public Procurement Procedures, Commissioner for Protection of Equality, etc. Each of the aforementioned bodies performs control of the security system defined by the law that regulates the work of an independent and independent body.

Supervision and control of the security sector is also carried out by civil society, through civil society organizations, experts, researchers, representatives of the academic community and others who can participate in discussions and debates on issues related to security. Citizens' associations and research institutions can conduct independent research on the operation of the security system, monitor respect for human rights in the security system, inform the public about issues that are important for the entire society, educate professionals and the general public about the operation of the security system, provide feedback on various decisions made in the security system (Kekovic & Dimitrijevic, 2017). In addition, the role of public information is also important. Through the means of public information, citizens can exercise their right to information about matters of public importance.

State security entities implement mechanisms of internal control and supervision, in order to ensure adherence to high standards in the provision of security by their members. Control mechanisms include internal disciplinary measures, measures of supervision and audits of work by lines of command and leadership. Subjects of internal control can be controlled and

supervised by independent and autonomous state bodies, as well as by the management part of the security structure of the security system.

5. CONCLUSION

The Constitution, international treaties, legal and by-laws, which refer to security issues in the broadest sense, as well as all special regulations on defense, police, security services, etc., prove that security is fundamentally indivisible, even though it is regulated by different laws and established under the jurisdiction of various state authorities. The security system of the Republic of Serbia is a normatively regulated, structural and functional unit of competent state bodies, state administration bodies, security and intelligence systems, as well as other entities whose activities contribute to the protection of the vital values of the Republic of Serbia and its citizens. The security system is legally regulated by: the Constitution, the National Security Strategy, the Defense Strategy and laws that directly or indirectly regulate the security system of the Republic of Serbia. The national security strategy is the highest strategic document and represents the starting point for the preparation of all other documents of importance for the security system.

Security system control is one of the important elements. The importance of the control of the security sector is reflected in the improvement of the security situation, that is, the prevention, suppression and remediation of the consequences caused by the illegitimate and illegal performance of the security function. Full control of the work of elements of the National Security system is legally established by the above-mentioned laws and entrusted to various state and non-state bodies.

REFERENCES

Constitution of the Republic of Serbia. (2021). Official Gazette of RS, no. 98/2006 and 115/2021.

Defense Law (2018). Official Gazette of the RS, no. 116/2007, 88/2009, 104/2009, 10/2015 and 36/2018.

Defense Strategy of the Republic of Serbia (2019). Official Gazette of the RS, no. 94.

Dragisic, Z. (2011). National Security System of the Republic of Serbia, Faculty of Security, Belgrade.

Djukic, S. (2017). Military act, Basics and security system in national security strategy, Vol. 69 (No. 7), ISBN 0042-8426

Hadzic, M. (2012). Parliamentary control and supervision of the security sector of Serbia, OSCE Mission in Serbia/Belgrade Center for Security Policy, Belgrade.

Hadzic, M. Milosavljevic, B. (2013). Legal structure of the Serbian security sector, Belgrade Center for Security Policy, Belgrade.

Hadzic, M. Stojanovic-Gajic, S. (2012). Yearbook of security sector reform in the Republic of Serbia 2008-2011, Belgrade Center for Security Policy, Belgrade.

Kekovic, Z. (2009). Security Systems, Faculty of Security, Belgrade.

Kekovic, Z. Dimitrijevic, I. (2017). Security systems with the security system of the Republic of Serbia, University of Belgrade, Faculty of Security, Belgrade.

Kovac, M. (2003). Strategy and doctrinal documents of national security, The world of books, Belgrade.

Law on the Basics of Organizing the Security Services of the Republic of Serbia (2012). Official Gazette of the RS, no. 116/2007 and 72/2012.

Mijalkovic, S. (2018). National Security, Criminal Police Academy, ISBN 978-86-7020-402-7 Belgrade.

Military Lexicon. (1981). Military Publishing House, Belgrade.

National Security Strategy of the Republic of Serbia (2019). Official Gazette of the RS, no. 94.

Rules of Procedure of the National Assembly of the Republic of Serbia Available from [http://www.parlament.gov.rs/narodna-skupstina-/vazna-dokumenta/poslovnik-\(precisceni-tekst\)/ceo-poslovnik-\(precisceni-tekst\).1423.html](http://www.parlament.gov.rs/narodna-skupstina-/vazna-dokumenta/poslovnik-(precisceni-tekst)/ceo-poslovnik-(precisceni-tekst).1423.html) Accessed: 03.08.2023.

Stajic, Lj. (2021). Basics of the security system, Faculty of Law in Novi Sad, ISBN 978-86-7774-242-3, Novi Sad.

Vujaklija, M. (1980). Lexicon of foreign words and expressions, Education, Belgrade.

CURRENT STATE OF EMERGENCY MANAGEMENT IN THE REPUBLIC OF SERBIA

Jovanka Tosic^{1a}, Zorana Ivetic^{2b}

¹ Educons University, Faculty of Security Studies, Vojvode Putnika 87, Sremska Kamenica, Republic of Serbia jovanka.tosic@educons.edu.rs

² Educons University, Faculty of Security Studies, Vojvode Putnika 87, Sremska Kamenica, Republic of Serbia, zorana.ivetic@educons.edu.rs

Received: 2th August 2023

Accepted: 16th August 2023

Professional paper

Abstract: *An emergency situation represents a complex combination of events, in which there was an irregular state of functioning of the social system or its parts. Caused by events of a larger scale, emergency situations have the effect of endangering the population, material goods and the environment, thus putting to the test the ability of society and the state to react successfully in unforeseen circumstances.*

It is necessary to undertake comprehensive measures in order to manage emergency situations. Successful management of emergency situations requires cooperation and coordination of all participants in the system, at the level of the Republic of Serbia, at the level of the Autonomous Provinces and at the level of local self-governments, in order to mitigate the consequences of the emergency situation and ensure the fastest and most efficient recovery.

The paper analyzes the current state of emergency management in the Republic of Serbia. Procedures and institutions dealing with responding to emergency situations in the Republic of Serbia were analyzed. The inductive-deductive method as well as the method of content analysis was used.

Key words: *emergency management, legal framework, emergency headquarters, emergency situations*

1. INTRODUCTION

Emergency situations represent a complex combination of different events. They put to the test the ability of society and the state to react successfully in such unforeseen circumstances. This term is often used in the current context by different people and media.

At the same time, a state of emergency is a situation when threats to the population, the environment and material goods are of such a scale that their occurrence cannot be prevented by the regular action of the competent authorities and services, which is why it is necessary to

^a ORCID: 0000-0001-6025-3542

^b ORCID: 0000-0003-0629-8189

use special measures, forces and means to mitigate and eliminate them with a strengthened regime work.

Regardless of the increasing frequency of such situations, it is becoming increasingly important to take comprehensive measures in order to manage emergency situations in the Republic of Serbia. This includes an analysis of the current state of emergency management in the Republic of Serbia, an analysis of the procedures and institutions that deal with responding to emergency situations at different levels in the Republic of Serbia.

Emergency management is a complex and challenging process that requires a well-organized and coordinated management system. Successful management of emergency situations implies an efficient and effective response in the most domestic conditions, which is possible only if the entire system is functioning.

Successful management of emergency situations requires cooperation and coordination of all participants in the system, at the level of the Republic of Serbia, at the level of the Autonomous Province and at the level of local self-government, in order to maximize the impact on preventing, minimizing and mitigating the consequences of disasters and emergency situations, and to ensure the fastest and more effective recovery in case such situations occur.

2. LEGAL FRAMEWORK OF EMERGENCY SITUATIONS IN THE REPUBLIC OF SERBIA

Every emergency situation, regardless of its source and consequences, affects the activities of individuals, organizations, local communities and even society as a whole. In order to avoid social disorganization that can lead to undesirable events, it is important to define such situations through legal acts.

The meaning of the term "legal framework" includes the system of laws, regulations, regulations, court decisions and other forms of legal norms whose purpose is to regulate relations between people and society. In the Republic of Serbia, emergency situations are regulated by law. The basis of the regulation is the Constitution of the Republic of Serbia and the Law on Reduced Disaster Risk and Emergency Management (Law on Disaster Risk Reduction and Emergency Management, 2018.).

It is very important that there is an adequate legal framework that will establish an effective response system in case of emergency situations. In the text that follows, the documents of the legal framework of emergency situations will be presented, as well as the emergency management regulations in the Republic of Serbia.

When it comes to the Republic of Serbia, the most important laws are: Law on Disaster Risk Reduction and Emergency Management (Law on Disaster Risk Reduction and Emergency Management, 2018), Law on Fire Protection (Law on fire protection, 2018), Law on Reconstruction after Natural and Other Disasters (Law on reconstruction after elementary and other disasters, 2015), Regulation on the implementation of evacuation (Regulation on implementation of evacuation, 2011).

All the above-mentioned documents and regulations should ensure fast, efficient and coordinated action in case of emergency situations, as well as protect the lives, health and safety of citizens and property in those situations.

The basic law that regulates the field of emergency situations in the Republic of Serbia is the Law on Disaster Risk Reduction and Emergency Management. This law establishes the basic rules and principles of management in emergency situations, including the way of organization, work and relations of competent authorities in these situations.

In 2018, the National Assembly of the Republic of Serbia passed the Law on Disaster Risk Reduction and Emergency Management. The law regulates disaster risk reduction, prevention and strengthening of resilience and readiness of individuals and communities to respond to the consequences of disasters, protection and rescue of people, material, cultural and other assets, rights and obligations of citizens, associations, legal entities, bodies of local self-government units, autonomous provinces and the Republic of Serbia, management of emergency situations, functioning of civil protection, early warning, notification and warning, international cooperation, inspection supervision and other issues of importance for the organization and functioning of the disaster risk reduction and emergency management system (Law on Disaster Risk Reduction and Emergency Management, 2018).

According to the above-mentioned law, the risk assessment must be made by the Republic, the province, units of local self-governments, companies, health institutions, as well as educational institutions. On the other hand, the disaster risk reduction plan must be adopted by the Republic, the province, as well as the local self-government units.

3. MANAGEMENT OF EMERGENCY SITUATIONS

Natural disasters pose a threat to human communities, whether it is a local, regional or global level of threat, therefore society was forced to develop appropriate protection mechanisms. In the past, people did not have solutions to deal with these threats, which resulted in the devastating consequences of natural disasters, great loss of life and severe property damage. However, the state recognizes the importance of protection and has developed appropriate emergency management mechanisms to minimize possible catastrophic consequences (Prelic, 2023).

The management of emergency situations requires the identification of possible emergency events, the formation of scenarios for the development of these events, the analysis of the mutual conditioning of events and their consequences, the analysis of the impact of various environmental risk factors (e.g. the analysis of dangerous objects in the environment), as well as the taking of appropriate preventive measures to minimize or eliminate the possibility their occurrence, i.e. operative and remedial measures in the event of the realization of these events. Environmental hazard factors are extremely important for successful emergency management because they can increase the negative consequences of emergency situations (Stoimenov et al., 2013).

Management in emergency situations is the guidance of protection and rescue entities in the performance of obligations and tasks to improve the security system in an extraordinary and destabilized state of society caused by large-scale events that paralyze the functioning of the social system (Ljustina & Knezevic, 2013).

For the coordination and management of protection and rescue in emergency situations in accordance with the Law on Disaster Risk Reduction and Emergency Management and other regulations, emergency headquarters are formed as operational and expert bodies and that: For the territory of the Republic of Serbia - Republic Headquarters for Emergency Situations, formed by the Government; For the territory of the autonomous province – the provincial headquarters for emergency situations, which forms the executive body of the autonomous province; For the territory of the administrative district - the district headquarters for emergency situations, which forms the Republic Headquarters for emergency situations; For the territory of the city - the city headquarters for emergency situations, which educates City Assembly; For the territory of the municipality - the municipal headquarters for emergency situations, which educates municipal assembly (https://www.divac.com/upload/document/podsetnik_preview.pdf).

The involvement of headquarters at different levels aims at effective coordination and management in emergency situations, as well as a quick reaction and response to various challenges that may arise. These headquarters work in cooperation with various sectors and institutions, including the police, military, ambulance, fire service, health facilities, in order to effectively respond to emergency situations and protect citizens.

3.1. State of emergency management at the level of the Republic of Serbia

In the Republic of Serbia, the Government is responsible for all aspects of emergency management. In its name, the responsibility for planning and implementing preventive measures, preparedness, response to emergency situations and elimination of their consequences, was transferred to the joint activity of competent state administration bodies, autonomous provinces and local self-government units. The responsibilities of each of the listed entities are defined by the Law on Disaster Risk Reduction and Emergency Management (Law on Disaster Risk Reduction and Emergency Management, 2018).

In the Republic of Serbia, citizens in emergency situations cannot call a single number for all emergency services, but each emergency service is called on a separate number that differs from service to service. Unfortunately, coordination between dispatch centers is not always effective, which can lead to delays in responding to emergency situations. Also, the current system of identifying and locating callers is not sufficiently developed, which makes it even more difficult for emergency services to respond quickly and accurately in situations where every second counts. In order to improve the situation, it is necessary to develop a better database for monitoring all kinds of hazards, events, emergencies and disasters, as well as to improve the existing system of coordination of emergency services.

The national emergency protection and rescue strategy, which was published in 2011 and expired in 2021, stated that a universal emergency call system called "Number 112" would be introduced. However, this system was not implemented (National strategy for protection and rescue in emergency situations, 2011).

The introduction of that universal system "Number 112 for emergency calls" was supposed to achieve synchronization, quick and efficient response in emergency situations, disasters and other emergency events. This system includes advanced operational procedures, technologically advanced equipment, increased readiness and trained personnel in accordance with European standards.

As pointed out by the authors Karovic, Domazet and Jesic „[...] a particular problem in the Republic of Serbia is that there is no strong public sector, nor is there a well-developed welfare state and open and transparent work at all levels of executive power, including the government.[...] The mentioned authors also state that citizens' trust in local self-government is different, and that the relationship of mutual trust between state bodies is possibly less than in other countries (Karovic et al., 2021).

The effective functioning of the protection and rescue system depends on the quality of human resources and the equipment of the services for preventive and operational response. Unfortunately, the analysis of the current situation shows that both human resources and equipment are not at a satisfactory level. These resources are equally essential and elementary for the successful functioning of the protection and rescue system. Therefore, it is necessary to make an additional effort to improve the quality of human resources and the equipment of the services, so that the protection and rescue system is more efficient and better prepared for any possible situation.

3.2. State of emergency management at the level of the Autonomous Province of Vojvodina

Based on the research conducted as a result of project no. 142-451-2675/2018-1 dated 07/04/2018. regarding the vulnerability of local self-governments to floods in the territory of AP Vojvodina, where the following local self-governments are included in the survey: Secanj Odzaci, Pancevo, Beocin, Sremska Mitrovica, Becej, Apatin and Backa Palanka, Karovic and Domazet state that, „[...] it is characteristic that the conditions in local self-governments are quite similar and that there are no significant differences. In particular, it can be observed that the local governments, which were taken as a sample, are threatened by floods and that floods are caused by heavy rains and groundwater and that groundwater causes the greatest damage. Floods occur cyclically at intervals of more than 10 years, most often during the months of May and October, but that is not the rule. They can also appear in other months of the year (Karovic & Domazet, 2019).

In particular, it should be emphasized that the damage caused by floods in the local self-governments of AP Vojvodina most often affects agricultural arable land, but urban areas are not spared either. It should be emphasized that, when it comes to preventive measures within local self-governments, especially in connection with flood prevention, the sewage network has not been built at a sufficient level. Also, the built embankments are not of sufficient length or height and are not always functional to prevent flooding.

As stated by the authors Karovic and Domazet „[...] floods that occur in local governments in the area of AP Vojvodina threaten the life and health of the population, property, road and rail traffic, infrastructure for water and electricity supply, sewerage and the telecommunications system are at risk. Although, according to the recorded situation, there is a flood monitoring system in local self-governments, it is not at such a level that it can at any moment provide essential information regarding the flood situation and possible timely measures. This is the weakness of such organized monitoring in relation to the upcoming dangers of possible floods (Karovic & Domazet, 2019).

Based on the recorded situation in local self-governments in the area of AP Vojvodina, it can be concluded that floods are one of the main problems that these self-governments face. Heavy rains and underground water threaten almost the entire area, and the built sewage network is not fully ready to receive such amounts of water. Irregular maintenance and lack of financial resources contribute to endangering the sewage network, and the low level of awareness of the population about the need for preventive action further complicates the situation.

This attitude towards floods is harmful, because floods do not occur often, and their impact can be extremely destructive. Therefore, it is important to invest in taking measures that would prevent floods, and this includes maintaining the sewage network on a regular basis and increasing the population's awareness of the importance of preventive measures.

3.3. The state of emergency management at the local self-government level

The local self-government unit is responsible for, through its organs, and in accordance with the Constitution of the Republic of Serbia, the Law on Local Self-Government and the Law on Disaster Risk Reduction and Emergency Management, to take care of environmental protection, to adopt programs for the use and protection of natural values and environmental protection programs, and to organize protection from natural disasters and other major disasters, as well as fire protection, and to create conditions for their elimination, i.e. mitigation of their consequence (https://www.divac.com/upload/document/podsetnik_preview.pdf).

As stated in the Methodology for preparation and contents of disaster risk assessment and protection and rescue plan, the plan of the local self-government unit is prepared for the territory of the local self-government unit and contains: early warning and preparedness (readiness); mobilization and activation; protection and rescue by types of danger; external plan for protection against a major accident (if there is a higher-order SEVESO complex on the territory of the local self-government); civil protection measures (warning, evacuation, sheltering, treatment, first and medical aid and field sanitation) and the use of protection and rescue forces and subjects (Methodology for preparation and content of disaster risk assessment and protection and rescue plan, 2019).

Local self-government through the protection and rescue plan should have clearly defined procedures and responsibilities for the work of all bodies and their precise implementation. Based on the treatment of data found in the database of the implemented project entitled: "Model of functioning of local self-government in emergency situations (flood)" no. 142-451-2675/2018-01/01 from July 4, 2018. collected data show: that the organization of local self-government bodies is directly related to the functioning in case of emergency situations caused by floods.

Based on the data from the above-mentioned project, it can be noted that the characteristic elements are primarily manifested in the segments related to the response of local self-government bodies in emergency situations, the existence and functioning of the headquarters for emergency situations caused by floods and the agreed procedure for requesting assistance from the competent authorities at the level of the District and Autonomous provinces.

Considering the state of local self-governments in relation to the organization of local self-government in emergency situations, it is not possible to speak with high reliability about the level of organization, primarily if it is taken into account that many issues have not been resolved in an efficient manner. There are partially plans to check the functioning of local self-government in emergency situations, but this should also be taken with a grain of salt, while the common assessment is that the approved financial resources are not sufficient for local self-government bodies to function successfully in the conditions of an emergency situation caused by floods (Karovic & Domazet, 2019).

Based on all of the above, it can be concluded that the level of organization of local self-government in the event of an emergency situation does not instill much confidence, especially in segments that deal with problems of a financial nature, and mostly of a professional nature. The main challenges are insufficient quality of staff, limited financial resources, unrealistic planning and lack of engagement in solving the flood problem.

Part of the research on the mentioned project refers to the plan of protection and rescue and its functionality, where it can be noted that plans have been made in some local governments, while in most others they are still not available. As the reason for this deficiency, it is stated that the dates ordered by the competent authorities for the preparation of the plans were too burdensome and that the local self-governments had inertia in relation to their preparation. In addition, there is a lack of professional bodies capable of preparing these plans, and the responsibilities of persons and competent bodies for their preparation are not clearly defined.

From the aforementioned research, it can be concluded that in many local governments, protection and rescue plans are often neglected and not sufficiently updated on an annual basis. This can be a risk because the plans do not reflect the actual situation and the actors involved may not be aware of their obligations and responsibilities. In addition, in some cases, plans are drawn up, but they are not sufficiently functional and serve only as a paper formality. These

weaknesses are present in most local governments and attention needs to be paid to this problem in order to strengthen the protection and rescue capacity at the local level.

Based on the situation in local self-governments and an overview of the activities and development of the disaster risk reduction system, a special part that should be focused on is the technical and technological equipment of local self-government, which is necessary for effective action in emergency situations. In the current state, local self-governments do not have sufficient technical and technological equipment, nor adequate means with which they can react in similar situations.

Funding of the protection and rescue system is extremely important, considering that the level of equipment and the speed of response of rescue teams in emergency situations decisively affects the scope and severity of the consequences of certain extraordinary events, that is, the amount of material and any other damage.

4. CONCLUSION

Emergency situations, which are defined in the legal framework of the Republic of Serbia, cause various damages to the social community. The legal framework of emergency situations in the Republic of Serbia defines key elements and responsibilities in such a situation. The declaration of a state of emergency can be caused by various events, such as floods, fires, earthquakes, explosions or other disasters caused by the action of nature or the human factor. All of this requires that society, that is, the state, should be prepared to be able to react in such a situation and organize itself to be able to manage an emergency situation. This means that it is capable of enabling the protection and rescue of the population and material goods in such conditions.

Effective disaster risk reduction and emergency management depends on the quality of human resources and the equipment of the services for preventive and operational response. Unfortunately, the analysis of the current situation shows that both human resources and equipment are not at a satisfactory level. These resources are equally essential and elementary for the successful functioning of the protection and rescue system. Therefore, it is necessary to make an additional effort to improve the quality of human resources and the equipment of the services, so that the protection and rescue system is more efficient and better prepared for any possible situation.

In the paper, it was determined that in the area of AP Vojvodina, floods are one of the main problems that these self-governments face. Although there is a flood monitoring system implemented in local self-governments, it is insufficiently developed to provide comprehensive information on the current flood situation and enable timely taking of adequate measures. This represents the weakness of such organized monitoring in terms of anticipating possible floods and implementing the necessary actions on time.

It can be stated that the level of organization of local self-government in the event of an emergency does not instill much confidence, especially in the segments that deal with problems of a financial nature, and above all of a professional nature. The main challenges are insufficient quality of staff, limited financial resources, unrealistic planning and lack of engagement in solving the flood problem. The lack of engagement may stem from the fact that floods occur sporadically and are not always an actual problem.

REFERENCES

Karovic, S., Domazet, S. (2019). The functioning of local self-government in emergency situations, Educons University, Sremska Kamenica

Karovic, S., Domazet, S. Jesic, J. (2021). Local self-government in the conditions of a pandemic crisis, Educons University, Sremska Kamenica

Law on Disaster Risk Reduction and Emergency Management (2018). Official Gazette of the the Republic of Serbia no. 87/18.

Law on fire protection (2018). Official Gazette of the the Republic of Serbia, No. 111/2009, 20/2015, 87/2018 and 87/2018 - others. laws.

Law on reconstruction after elementary and other disasters (2015). Official Gazette of the the Republic of Serbia, No. 112/2015.

Ljustina, A. Knezevic, N. (2013). Emergency situations caused by natural disasters, *Ecologica* 20, (No.71)

Methodology for preparation and content of disaster risk assessment and protection and rescue plan (2019). Official Gazette of the the Republic of Serbia, No. 80/2019

National Strategy for Protection and Rescue in Emergency Situations (2011). Official Gazette of the the Republic of Serbia, no. 86/2011.

Prelic J. (2023). The role of local self-government units in entrepreneurship measure for remediation consequences of the earthquake, Available from <http://www.va.mod.gov.rs/multimedia/zavrsni%20rad%20Prelic%20Jovan.pdf> Accessed: 2023-07-27.

Regulation on implementation of evacuation (2011). Official Gazette of the the Republic of Serbia, No.22/2011.

Stoimenov, L., Stanimirovic, A., Milosavljevic, A., Zivkovic, P. (2013). Management of emergency situations using GIS technologies.

https://www.divac.com/upload/document/podsetnik_preview.pdf Accessed: 25.05.2023.

MILITARY APPLICATION OF ARTIFICIAL INTELLIGENCE

Milan Miljkovic¹, Hatidza Berisa^{2a}, Srdjan Zgonjanin³

² University of Defence in Belgrade, Veljka Lukica Kurjaka 1, Belgrade, Republic of Serbia,
milanmiljkovic04011@gmail.com

² University of Defence in Belgrade, National Defense School, Veljka Lukica-Kurjaka 33,
Belgrade, Republic of Serbia, hatidza.berisa@mod.gov.rs

² University of Defence in Belgrade, Veljka Lukica-Kurjaka 1, Belgrade, Republic of Serbia,
srdjanzgonjanin007@gmail.com

Received: 4th August 2023

Accepted: 10th August 2023

Original scientific paper

Abstract: *The application of artificial intelligence for military purposes can be broadly divided into three main areas. The first area involves enabling weapons and military equipment to operate without human supervision. The second area focuses on the processing and interpretation of large amounts of data, which aids in intelligence work, defining military strategy, and making strategic decisions. The third area pertains to assisting military systems in executing commands and observations independently during combat situations. AI applications offer armed forces a competitive advantage by accelerating decision-making through transforming the OODA decision-making loop, enhancing overall command capability. As the technology evolves, the "unpredictable, fragile, inflexible, and inexplicable characteristics of artificial intelligence" remain to be fully understood, allowing it to continue surpassing strategy and human error. However, like any revolutionary technology, artificial intelligence is likely to intensify competition among militarily powerful states, leading to a security dilemma that increases the potential for escalation.*

Key words: *artificial intelligence, decision making, challenges*

1. INTRODUCTION

The massive influx of information, coupled with rapid technological advancements, is transforming the nature of modern warfare. In the information age, data becomes a critical component of national power, and those who are best informed will gain strategic superiority through improved decision-making and increased efficiency. Artificial intelligence (AI) will play a pivotal role in reshaping the OODA loops (decision-making loops) in the digital age and will be at the core of commanding military operations. By applying AI to conventional capabilities, decision-making can be accelerated, enabling warfare at machine speed and surpassing human cognitive abilities. As the technology continues to mature, AI is already shaping military doctrine and defining future strategies.

^a ORCID: 0000-0002-9432-5273

Despite the potential advantages in military applications, artificial intelligence also presents specific challenges. It can be susceptible to unique forms of manipulation. When AI augments conventional military capabilities, it has the potential to destabilize strategic stability and disrupt the current global balance of military forces among great powers. This may exacerbate the "fog of war," unintentionally escalating conflicts, and increasing the likelihood of nuclear confrontations.

2. BASICS OF ARTIFICIAL INTELLIGENCE

The term "artificial intelligence" was first mentioned in 1956 at a scientific meeting in the USA, organized by the American computer scientist John McCarthy. The further development of artificial intelligence has been marked by ups and downs and periods of stagnation. However, at the beginning of the 21st century, there was a breakthrough in this area, primarily due to the increased possibilities of computer information processing and easier access to ever-increasing amounts of data.

Although artificial intelligence is not a new concept, its development has been accelerating in the 21st century, and scientists continuously revise its definition. For the purposes of this paper, we can use the widely accepted definition from the professional bodies of the European Union, which states that "artificial intelligence (AI - Artificial Intelligence) refers to systems that exhibit reasonable, intelligent behavior based on the analysis of their environment and make decisions - with a certain degree of autonomy - to achieve concrete goals" (AI development strategy in the Republic of Serbia, 2020-2025).

It is important to understand that artificial intelligence is the ability of computer systems to perform tasks that require human intelligence. Currently, artificial intelligence surpasses human intelligence in performing a narrow set of specific tasks. However, further research is needed to achieve artificial superintelligence, where machines' abilities exceed human cognitive ability (Sweijts, 2018). In the context of artificial intelligence, the term "artificial" refers to an inanimate being that performs intelligent actions, imitating natural intelligence, which is a characteristic of humans and other living beings.

What makes artificial intelligence intelligent is its ability to apply logical rules and principles established by the human mind, and also its machine learning capability. However, artificial intelligence falls short in achieving self-awareness – the awareness of one's own identity and what distinguishes a person from others. The global recognition of AI as a strategic technology and a valuable asset for exercising power and influence on the international stage has triggered a global race for supremacy in the AI economy and military affairs.

Major world powers have already announced their artificial intelligence development programs. In July 2017, the Government of the People's Republic of China announced a strategy with the aim of becoming a global leader in the field of artificial intelligence by 2030. In September 2017, Vladimir Putin announced Russia's intention to develop artificial intelligence, with the ambition of becoming a global leader in this field.

In January 2018, the US national defense strategy identified artificial intelligence as one of the key technologies that will "ensure that the US can fight and win the wars of the future." The US military has already integrated artificial intelligence systems within the "Project Maven," which was used to identify insurgents in Iraq and Syria.

3. ARTIFICIAL INTELLIGENCE IN CURRENT MILITARY ACTIVITIES

Military organizations consider Artificial Intelligence (AI) as a family of general-purpose technologies that enable machines to perform tasks typically requiring human intelligence or biological intelligence. AI plays a significant role in various military applications, with some

notable areas influencing the strategy of using military forces (Defence Artificial Intelligence Strategy, 2022).

In the realm of enemy *target detection and recognition*, AI techniques can enhance the accuracy of target identification. Intelligent systems can predict enemy activity and aggregate combat environment data. Machine learning is used to track targets and collect data, and AI plays a crucial role in intelligence and reconnaissance applications, mainly due to its ability to analyze large datasets. The US Army's Project Maven is an example where AI automates intelligence data processing for counter-terrorism campaigns. Computer vision and machine learning algorithms are used to analyze drone footage, identifying enemy activities for intelligence and targeting purposes. This automation can save human analysts significant time and enable more efficient decision-making based on collected data. The intelligence community, particularly the Central Intelligence Agency, is actively engaged in developing around 140 projects involving AI for tasks like image recognition and predictive analytics. These efforts encompass language recognition, speech translation in noisy environments, geolocation image analysis without metadata, and the development of building function identification tools based on lifestyle pattern analysis.

In the context of *combat environment awareness and reconnaissance*, unmanned systems equipped with AI can follow predetermined routes to enhance threat assessment and situational awareness. Combining unmanned aerial vehicles and AI facilitates border monitoring and threat identification, leading to faster response times.

Artificial Intelligence significantly *contributes to strategic decision-making* by improving the accuracy and speed of conflict scenario analysis, eliminating biases in decision-making, and enabling rational choices during urgent situations.

To enhance the *command and control of military forces*, the US aims to utilize AI's analytical potential. The development of a multi-domain command and control system by the American Air Force seeks to centralize planning and execution of operations across various domains (air, space, cyber, maritime, and ground). AI could merge sensor data from these domains to create a comprehensive "common operating picture" for decision-makers.

However, there are *some limitations and challenges* associated with AI in military use. Strategic decision-making using AI can negatively impact stability during crisis situations due to rapid assessments and decisions. Decision-making algorithms can be biased and susceptible to adversarial influence. In military operations, problems may arise, including supply chain risks, uncertainty about using automated vehicles in complex situations, and the high cost of implementing AI. The complexity of engineering involved in creating AI-equipped weapon systems, along with high maintenance costs, pose significant obstacles, especially in wartime conditions.

4. ARTIFICIAL INTELLIGENCE AND STRATEGIC DECISION-MAKING

What sets artificial intelligence apart as a world machine is its autonomy in executing John Boyd's OODA loop (Observe-Orient-Decide-Act), i.e., independence on the battlefield, consisting of observing the environment, orienting one's own position in relation to all important elements of the environment, making a decision on executing an action, and taking action itself. The primary conceptual differences in the application of artificial intelligence in military affairs relate to the role of humans in the decision-making loop, whether they are "in the loop" (HITL concept - Human-In-The-Loop) or "on the loop" (concept of Human-On-The-Loop). If a person ultimately decides on "pulling the trigger" it is a matter of supervised autonomy, while leaving that right to the machines implies full autonomy (Sar, 2020). The application of artificial intelligence to conventional military capabilities has the potential to

speed up decision-making, enable warfare at machine speed, and surpass human cognitive abilities. Already, AI significantly shapes military doctrine and will continue to define future strategy as the technology matures (Lastovych, 2021).

Early studies suggest that AI will be useful both at the tactical and strategic levels. However, on the strategic decision-making level, there might be more ambiguity about data and the rewards each machine aims to achieve. The immediate role of artificial intelligence may be in the tactical domain, but it will still have significant strategic implications (Kenneth, 2018).

In addition to its strategic effect through tactical victories, AI will also shape strategy by providing insights to decision-makers based on the processing of vast datasets. Strategic-level AI can act as a "prophet" for decision-makers, testing and rejecting false associations and assumptions about adversaries, and identifying key vulnerabilities in the enemy. Strategic AI will be free from the individual and collective psychological processes influencing human decision-making, such as groupthink, bias, bureaucratic politics, excessive optimism, and poor risk assessment.

To enhance accurate decision-making and predict conflict scenarios, war games using artificial intelligence and advanced simulations can be employed. These measures theoretically support strategic stability.

However, the most challenging problems related to warfare are actually strategic problems, which involve uncertainty or the "fog of war," as famously noted by Clausewitz. In such unclear strategic situations, as Jon Lindsay, an associate professor in the School of Cyber Security and the Sam Nunn School of International Affairs, states, "human sense is needed to make moral, ethical, and intellectual decisions in an incredibly confusing, tense, and frightening situation."

Lindsay emphasizes that decision-making using AI is based on four key components: data on the situation, interpretation of that data (or prediction), determining the best way to achieve goals and values (or reasoning), and taking action. While machine learning has made predictions easier, data and human judgment are still valuable. In war, however, unbiased data is usually lacking, and judgments about goals and values are inherently controversial, making human intervention essential (Goldfarb & Lindsay, 2022).

The idea of substituting soldiers with automated systems to reduce reliance on human labor and enhance battlefield effectiveness is called substitution theory AI. However, Lindsay and Goldfarb argue that AI should not be seen as a replacement but rather as a supplement to existing human strategy. Machines are good at predicting, but they depend on data and judgment. The most difficult problems in war are information and strategy, which are challenging to fulfill in the unpredictable military environment. In war, a wealth of unbiased data is usually lacking, and judgments about goals and values are inherently controversial, but that doesn't mean it's impossible to address.

If AI replaces humans as the central decision-making element in war, it could lead to changes in the structure and hierarchy of military leadership. People will be responsible for designing and maintaining data systems and making political decisions. Adversaries will aim to compromise both data and judgment, making human intervention even more critical.

Lindsay and Goldfarb conclude that while AI can automate prediction, judgment and data remain crucial. They question when armies will automate judgment or whether some analyses and assessments cannot be automated. Hence, the adoption of tactical and strategic decisions by humans remains the most important aspect of warfare. However, the fact remains that making fast and correct decisions is a challenge for today's strategic military leaders. A method

of rapid decision analysis involves fully utilizing cognitive abilities, empirical intuition, and logical reasoning to guide the decision-making process. With the development of science and technology, reliance on scientific decision-making and group decision-making becomes "mainstream" in modern military management at the strategic level. Despite the use of technology and big data, intelligent decision-making will still depend on human experience and intuition to achieve accurate and quick decisions.

Practice has shown that in the absence of military experience from combat operations, joint decision-making has become the primary approach to commanding and leading military operations. With the advancement of science and technology, the art of war has gradually been replaced by the reliance on scientific and group decision-making, which has become mainstream, as evidenced by its application in the Gulf War, aggression against FRY, and conflicts in Kosovo and Metohija, Iraq, Afghanistan, Libya, Syria, and other regions (Xianjin & Qiwan, 2018). Traditional decision-making based on personal experience is no longer sufficient for military commanders. Instead, group decision-making highlights the advantage of collective wisdom, along with scientific decision-making, which relies on contemporary decision-making models and operational research. This has become the primary method of modern military management at the strategic level, thus enabling precise decision-making.

In traditional military decision-making, commanders relied on their own experience, intuition, and intelligence to make critical choices. However, the emergence of technology and big data tools has offered a new approach to decision analysis. Big data has shifted away from traditional reliance on experience and intuition, emphasizing the importance of data and analysis. This shift not only enhances the results of scientific decision-making but also alleviates the immense mental stress that decision-makers face. Intelligent decision-making is now liberated from human experience and intuition, mitigating the errors that can occur in human decision-making and allowing for accurate and swift decisions.

With this transformation in decision-making, the military can achieve more efficient and effective strategies. The fusion of scientific methods and big data enables decision-makers to make well-informed choices, leveraging collective insights and reliable analysis. As technology continues to evolve, the potential for even more sophisticated decision-making capabilities increases, further enhancing the military's ability to respond to complex and dynamic situations.

5. CHALLENGES OF MILITARY APPLICATION OF ARTIFICIAL INTELLIGENCE

However, the application of artificial intelligence in conjunction with nuclear or missile weapons, with their high range and destructive capabilities, goes beyond technological challenges and raises ethical considerations. Ethical and political guidelines dictate that decision-making should remain in the hands of humans, who must "pull the trigger" when circumstances demand it. Nonetheless, this perception may change as artificial intelligence technologies mature and become more reliable. Robert Work, the Deputy US Secretary of Defense, stated in 2016 that the US Department of Defense "will not delegate lethal authority to a machine to make a decision" regarding the use of force. However, he further elaborated that if adversaries with nuclear weapons, such as China or Russia, are more willing to entrust decision-making to machines than the US, then the US would have to consider how to best compete in such a scenario (Lamothe, 2016). This suggests that the United States might seriously contemplate removing the human element from the loop if their adversaries adopt autonomous decision-making. This willingness to engage in autonomous warfare is concerning, as it confirms predictions that AI could escalate friction, uncertainty, and instability in international security at the strategic level.

6. CONCLUSION

Artificial intelligence serves as a potent military force multiplier. Its applications can offer armed forces a competitive advantage by accelerating decision-making, transforming the OODA decision-making loop, and enhancing command, control, and supervision capabilities. However, until we fully comprehend the "unpredictable, fragile, inflexible, and inexplicable characteristics of AI," the technology will continue to surpass traditional strategies and human errors (Johnson, 2020). It is foreseeable that artificial intelligence, as a revolutionary technology, will intensify competition between nuclear-armed states, potentially leading to a security dilemma. The unpredictable nature of AI, coupled with an increasingly multipolar world order, may inadvertently trigger escalation and heighten the risk of conflicts. The immense potential of artificial intelligence could also introduce uncertainty into the international security landscape, disrupting the predictability of conflicts and increasing the likelihood of their escalation.

REFERENCES

- Defence Artificial Intelligence Strategy, (2022). v1.0, June 2022, UK Ministry of Defence (MOD), <https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy>
- Goldfarb, A. Lindsay, J. R. (2022). Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War. *International Security*; <https://direct.mit.edu/isec/article/46/3/7/109668/Prediction-and-Judgment-Why-Artificial>
- Johnson, J., S. (2020). "Artificial Intelligence: A Threat to Strategic Stability." *Strategic Studies Quarterly* 14, no. 1.
- Kenneth, P. (2018), „Artificial Intelligence: A Revolution in Strategic Affairs?“, *Survival, Global Politics and Strategy*, Published online: 18 Sep 2018.
- Lamothe, D. (2016). "The Killer Robot Threat: Pentagon Examining How Enemy Nations Could Empower Machines". *The Washington Post*. <https://www.washingtonpost.com>
- Lastovych, L. (2021). Artificial Intelligence's impact on future strategy, 05/14/2021 <https://www.defenceiq.com/air-land-and-sea-defenceservices/articles/artificial-intelligences-impact-on-futurestrategy>
- Xianjin B. Huang, Q. (2018). The Theories and Methods of Military Operations Research in BD&AI Era, Center for Assessment and Demonstration Research, Academy of Military Sciences, Beijing 100091, China, <https://www.atlantis-pess.com/proceedings/mmssa>.
- Strategy for the development of artificial intelligence in the Republic of Serbia for the period 2020-2025, <https://www.srbija.gov.rs/tekst/437277>
- Sweijjs, T. (2018). "Artificial Intelligence and Its Future Impact on Security" , Report, Hague Centre for Strategic Studies, <https://hcss.nl/report/testimony-from-timsweijjs-on-artificial-intelligence-and-its-future-impact-onsecurity/>
- Sar, P. (2020). *Vojska bez vojnika – autonomno oruzje i buducnost ratovanja*, Laguna, Beograd.

METHODOLOGICAL PROBLEMS OF DESIGNING RESEARCH IN SAFETY SCIENCES

Samed Karovic^{1a}, Jovanka Totic^{2b}, Zorana Ivetic^{3c}

¹ Educons University, Faculty of Security Studies, Vojvode Putnika 87, Sremska Kamenica, Republic of Serbia, samed.karovic@educons.edu.rs

² Educons University, Faculty of Security Studies, Vojvode Putnika 87, Sremska Kamenica, Republic of Serbia, jovanka.totic@educons.edu.rs

³ Educons University, Faculty of Security Studies, Vojvode Putnika 87, Sremska Kamenica, Republic of Serbia, zoranaivetic@yahoo.com

Received: 4th July 2023

Accepted: 31th July 2023

Review paper

Abstract: *Designing scientific research in the sciences of safety is essential for achieving quality results, efficient use of resources, protecting ethical principles and contributing to scientific knowledge in the field of security. The paper describes the elements of designing research in safety sciences with a focus on the research project for the preparation of the doctoral dissertation.*

Bearing in mind that the methodology of scientific research is the basis for successful conduct of scientific research, the emphasis is on the basic problems that arise when choosing research problems, defining research subjects, selection of samples, ethical issues, validity and reliability of data and interdisciplinarity.

These methodological problems are just some of the challenges that can be faced in the design of scientific research in the preparation of doctoral dissertations in the sciences of safety.

Key words: *methodology of scientific research, security science, research design, validity and reliability of data, ethical issues*

1. INTRODUCTION

Designing research in safety sciences is essential for defining research objectives, selecting the appropriate methodology, collecting relevant data, analyzing them and interpreting the results. Due to the specifics and characteristics of the safety sciences, the design of research requires and certain stages and steps, thus gaining the complexity and necessity of complying with established standards and procedures.

^a ORCID: 0000-0001-5470-4650

^b ORCID: 0000-0001-6025-3542

^c ORCID: 0000-0003-0629-8189

During many years of work and dealing with the methodology of scientific research, problems have crystallized in the design of research in the sciences of safety in the field of solving certain scientific problems that are often present with doctoral students and designing for the preparation of doctoral dissertations. The paper presents the basic elements of designing research with a focus on the scientific idea, and the key part that conditions other elements of scientific thought.

Also, the paper deals with the specifics of security sciences and their relationship with the most related sciences, primarily military and political sciences. This part is very important, because in research in the field of security sciences there are also "experts" from the aforementioned sciences, which makes it difficult to classify and mix certain problems in safety sciences. This is one of the issues that affects the number of scientists at certain institutions and whose views prevail in this case. But it's a special topic to consider on another forum.

The following specifically deals with the design of research in the sciences of safety and finally precisely defines the problems that are current in the field of designing research in the sciences of safety with some elements of guidelines that need to be in mind in order for design and research in the safety sciences to be scientifically verified and reflect the correctness of research and contribute to the development of safety sciences.

2. SECURITY SCIENCES

In the scientific ("Official Gazette of RS", 114/2017 and 24/2020) field of social sciences and humanities, they were classified as a security auxiliary and given the status of science. Bearing in mind the status of science, it should be noted, if the same as M. Markovic: "Science is objective, critical, methodically derived knowledge [...], whose goal is to establish the objective truth about reality." (Markovic, 1994) Markovic further points out, "in order to achieve this goal, science uses certain socially accepted research procedures and appropriate criteria for evaluating whether a particular research result should be accepted as true or not", (Markovic, 1994).

In this particular case, as M. Markovic pointed out again (Markovic, 1994), "the concept of knowledge (as well as the concept of truth) implies an object to which it relates and which is learned from a certain human perspective. In this case, every science has its own subject." Also, the concept of cognition implies a certain way of knowing, that is, a subjective practice by which one comes to the awareness of the object, which is the method", (Markovic, 1994).

Given the foregoing, the subject of security is the study and analysis of all aspects of security, including political, military, economic, social and technical dimensions. The aim of security education is to understand and understand the source and, nature and consequences of threats and challenges to security, as well as to develop strategies, policies and safeguards to ensure the safety of societies, organizations and individuals. In this sense, the sciences of security belong to the applied sciences "[...] which deal directly with practical problems and contain not only explanations of immediate experiential phenomena, but instructions for control and practical mastery of them. Most expressions of their language are descriptive, concrete, single or low degree of generality, methodologically, the focus is on technical data collection and classification, (Markovic, 1994).

From the point of view of the object of safety science, it can be concluded that it covers all aspects that are relevant to security, which includes international relations, military strategy, terrorism, crime, cybersecurity, global risks, crisis management, transport safety, energy, environmental protection and other areas that may have an impact on security. Precisely because of the width of the facility, the science of safety includes it and various disciplines and areas of research. The interdisciplinary approach is key to understanding and solving

complex security challenges, and security science will use knowledge in the fields of political science, international relations, military strategy, sociology, psychology, law, technology and other relevant disciplines.

In particular, it should be emphasized that security sciences have broader scope and are studied by various aspects of security at the global, national and individual levels. The science of security covers analysis of threats and challenges that threaten security, including terrorism, crime, cybersecurity, natural disasters, economic crises and other risk factors. At the same time, security sciences encompass multidisciplinary approaches in the fields of politics, law, sociology, psychology, technology and other disciplines in order to understand the nature of security challenges and develop strategies to overcome them. In this case, it is also important to note the relations between the sciences of security, military and political science.

1.1. The relationship between security sciences and military sciences

It is important to understand the relationship between military science and security sciences because both received classification at the same time. The subject of military science is primarily related to armed struggle. The sciences are a multidisciplinary field that deals with the study of military operations, strategies, tactics, technologies and organizations. The aim of military sciences is to understand and apply principles and concepts that are essential for military activities, including war planning, operations management, and military logistics. Include the study of historical conflicts, military theory, military doctrine, and the application of military technology. Their main orientation is on military operations and aspects that are directly related to armed struggle.

It should be noted that even if there are overlaps between military science and security sciences, military science is usually oriented towards the military aspects of security, while the sciences of security have a wider range of interests that include the civilian aspects of security. However, both fields can benefit from the exchange of knowledge, methodologies and experience, especially in areas such as crisis management, strategic planning, threat analysis and risk assessment.

In today's complex security environment, cooperation between military science and the sciences of security is becoming increasingly important in order to better understand and address contemporary security challenges and threats.

1.2. The relationship between security science and political science

What to keep in mind when it comes to political science and security science and how to make a distinction between them, it is necessary to look at the following:

1. Political sciences are mainly concerned with the study of political institutions, political processes, political systems, political theories, and political behavior. On the other hand, security sciences focus on the study of factors that affect national and international security, such as military strategy, terrorism, conflict, information security and the like.
2. When it comes to research, political science tends to understand political phenomena, processes, and systems in order to better understand political behavior and political decision-making. In contrast, security science studies the factors that influence security, in order to identify sources of threats, assess vulnerabilities, and develop protection strategies.
3. A particular aspect in the methodology of political science and security science research is that the political sciences use a variety of methodologies, including field research, political document analysis, interviewing, and statistical analysis. The security sciences

also use these methods, but often rely on intelligence analysis, security assessments, scenarios, and models.

4. A special relationship between these sciences is interdisciplinarity, which can be characterized in the fact that both political science and security science are areas that use concepts and approaches from other disciplines. Political science often relies on sociology, economics, philosophy, and history, while the sciences of security include elements of political science, international relations, military science, information security, and other related disciplines.
5. Finally, what should be particularly emphasized is that secretaires have a strong applied dimension, with the aim of providing guidelines for risk management, ensuring national security, implementing appropriate policies and decision-making. Political science, on the other hand, is often oriented to theoretical research and understanding of political phenomena.

So, these are key elements when it comes to the relationship between security science and political science, especially in the sphere of research. Unfortunately, in practice, it often happens that in the design and preparation of doctoral dissertations, the problem of research is replaced and the problems of political phenomena are classified into security problems and vice versa.

3.DESIGNING RESEARCH IN THE SCIENCES OF SAFETY

The design of research in the social sciences, which includes the science of safety, depends on the characteristics of the subject being researched. The subject of research in this area is so complex "[...] that it is not possible in scientific inquiry to include it in what is commonly called research methods", (Vujevic, 1983). The design of research involves meaningful, primarily mental activity in the development of a research project. As Milosavljevic M. points out, "it is a dynamically synchronized and coordinated system of interconnected and conditioned scientific and professional activities; mostly creative ones that are creating a research project", (Milosavljevic, 1980).

In this regard, the projection of research in the sciences of safety involves a series of steps that need to be carried out to define the problem of research, the subject of research, objectives and research, research hypotheses, method of research (methodology), collection of relevant data and analysis a Results. As a result of the design, a project is created that has its own characteristics, functions and parts.

The project is an imaginary model of [...] the acquisition of (scientific) knowledge about the subject of research, [...] it is an imaginary target, purposeful, rational and functional system and [...] a scientific and operational-organizational document" (Milosavljevic, 1980). In the end, it can be concluded that the project is an imaginary theoretical and practical model of acquiring scientific knowledge about the problem and the subject of research. It is, as The Merciful Says, "[...] expresses: first, idea – basic attitudes about the problem and subject of research; secondly – the idea of thought processes, techniques, means and procedures by which true scientific knowledge will be obtained", (Milosavljevic, 1980). It can be concluded that the design comes to the model, i.e. The whole we are [...] in their consciousness constructed and shaped on the basis of scientific and experiential knowledge, imagination, inspiration – through thinking according to the rules of logic. This model is expressed in appropriate language, signs, symbols, usually in writing and graphically in the form of a document called a research project", (Milosavljevic, 1980).

It should be noted, as Pointed out by Mihailovic D., "[...] The research project can be compared to a chess game. In it are firmly established the basic rules, what is the starting position of the figures, how they can move... [...] similar to a chess game and a research project is a kind of "mental game". There are well-known, generally accepted, firm rules by which research is conducted. The principles of methodological means and the order in their use shall be respected", (Mihailovic, 1999).

In order to understand research in the sciences of safety, it is important to present the structure of the entire research process. It is simply an established rule of research conduct methodology and is a consistent set of activities carried out during research in order to obtain objective, concrete and general and sufficiently critical and verifiable knowledge in the field in which the research is carried out. The research process is shown in Figure 1.

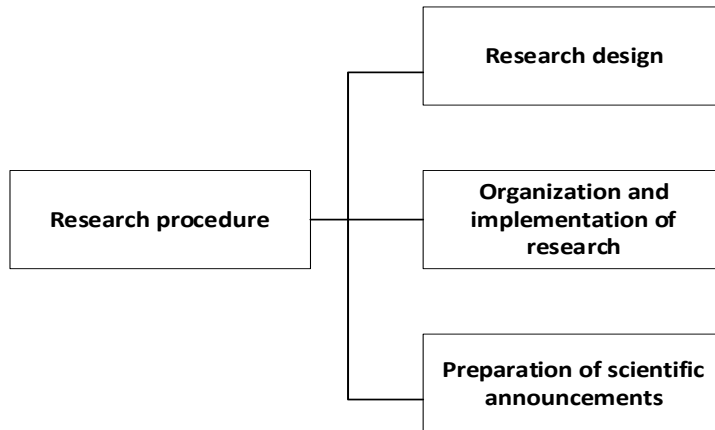


Figure 1. Research process
Source: Editing by authors

As you can see in the picture, the first element is the design of research. It should be emphasized that successful design in a particular area of research conditions fundamental knowledge in the theory and practice of a specific field, logic, methodology and other specific areas that are important for concrete research. As a result, a fully elaborated research project is created, the structure of which is shown in Figure 2.

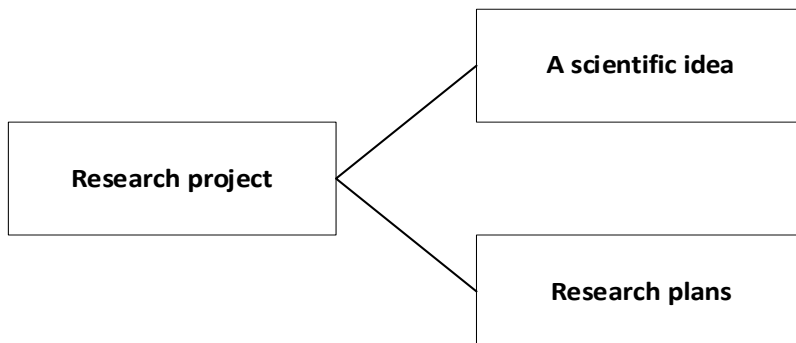


Figure 2. Structure of the research project
Source: Editing by authors

The paper is oriented on the scientific idea that is structurally shown in Figure 3. In this context, within the framework of the scientific concept, three key questions are answered:

1. What's being investigated?
2. Why is it being investigated and
3. How is it investigated?

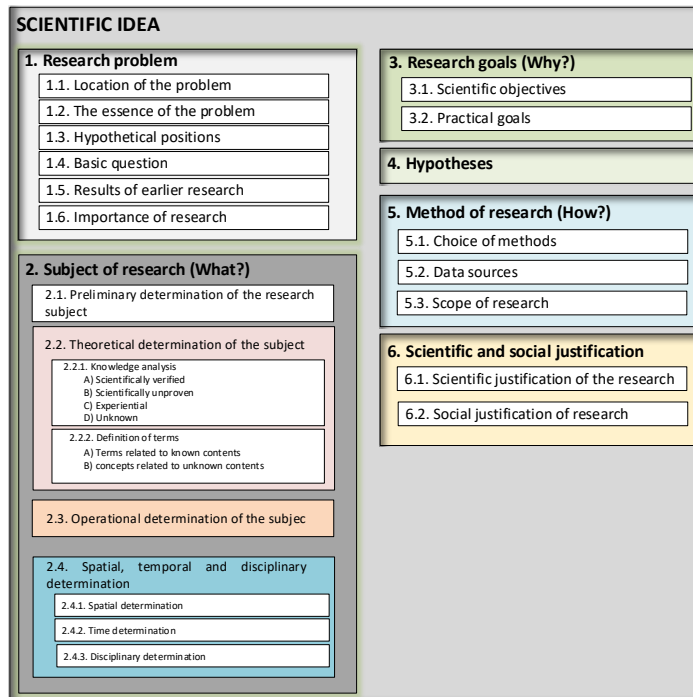


Figure 3. The scientific idea of research

Source: editing by authors

On each of the above questions, as pointed out by Milosevic N." [...] the answer is given through certain parts of the scientific idea" (Milosevic, 1989). The concept of designing research in the sciences of safety is that security is a term that refers to a state of freedom from risk, danger or adverse events. It refers to the protection of individuals, groups, organizations or states from potential threats or harmful influences. Security can be physical, psychological, financial, traffic, cyber, and many other types.

In particular, it should be borne in mind that security is a multidisciplinary area that studies the phenomena and factors that affect security and develops strategies, techniques and methods of protection. It uses knowledge and methodologies from various disciplines such as political science, sociology, psychology, technology, law, economics and information technology to analyze risks, identify potential threats and develop effective ways of responding. Discusses how to identify, analyze and manage various sources of danger in order to reduce the chances of damage or loss. It also explores how people, organizations and societies can prepare for emergencies, how to deal with them when they occur, and how to minimize their consequences.

All of the above elements have a complex impact on the design of research in the sciences of safety, especially on the design of research in the context of doctoral dissertations. The essence of the paper primarily refers to the design of research in the preparation of doctoral dissertations and the treatment of topics, the choice of research problems and the mixing of problems for which it is not necessary to "engage" science.

The methodology of scientific research has been in crisis for many years. Every mention of the methodology of scientific research carries the epithet that it is in crisis. It should be borne in mind that many scientists run away from the methodology of scientific research and that the biggest problems arise precisely in the design of research.

4. DESIGN AND RESEARCH PROBLEMS

On the problems of designing research in the sciences of security, we must first start from the fact that deduction safety (aka security science) is to be used in the field of safety. security science is a multidisciplinary field that studies the causes, factors and protection measures associated with safety. It deals with research, analysis and understanding of various aspects of security in order to identify risks and threats, develop appropriate protection models and strategies, as well as effective interventions to reduce or eliminate risks. It is precisely the stated property of the sciences of security that makes it difficult to design research, especially the selection and formulation of research problems, research objects, hypotheses, ways of research, data processing and the verification of hypotheses.

In particular, it should be noted that security sciences use various methods of research, data analysis, modeling, simulation and use of technological tools to provide effective strategies and solutions for the prevention, detection, response and recovery of security threats. It also deals with ethical, legal and political issues related to security.

The basic design problems in the safety sciences can be summarized as follows: defining the problem of research, selection of the sample, validity and reliability of the sample, the verification of hypotheses, ethical issues and interdisciplinarity.

The part concerning the design of research in the sciences of safety and which is the basis is the problem of research. As Zajecaranovic G. pointed out, "The problem is therefore a kind of question and it is the kind of questions that cannot be answered based on the available knowledge... Not all problems are scientific problems. The scientific problem is only that which contributes to the enrichment of scientific knowledge, that is, that problem which, when solved, contributes to the development of scientific knowledge" (Milosevic, 1989).

Thus, the draft of the scientific idea begins with the formulation of the research problem where the connection between the scientific-theoretical fund and the concrete research project is established. It contains a cross-section of pre-existing theories and significant research in the field of problems that are to be investigated (Mihailovic, 1999). This is one of the elements concerning design and which in the formulation of the research project bypasses and does not understand. That is why difficulties arise because the problem of research is often identified and confused with the subject of research. It should be noted that the problem of research is broader than the subject of research and surpasses other parts of the research project. Therefore, in security sciences, problems can often be complex and insufficiently precisely defined. That is why it is important to carefully formulate a research problem to ensure clarity and direction of research.

Of course, it should be further noted and ambiguities concerning hypotheses, their role in research, in particular, determining the level of scientific knowledge, indicators and instruments. The relationship between the importance of hypotheses in the research and testing of hypotheses in statistics is often identified, thus creating general confusion in the verification of hypotheses and the results of the research. All this affects the production of reports, their quality and essentially the results of the research.

When it comes to the assembly of the appropriate sample for research, it should be noted that it is done with a limited number of participants that may be difficult to reach, such as e.g.

soldiers, members of the police force or other special units. Such challenges can make it difficult to generalize survey results to the entire population.

Collecting relevant data in the sciences of security, or data science in general, is a challenging job that is conditioned by indicators and a built instrument. Limited access to information, inconsistency or unreliability of data, as well as their interpretation, can affect the validity and reliability of research results. Therefore, it is important to apply appropriate methods of data collection and analysis to ensure their accuracy and reliability.

It should be especially emphasized the method of verification of hypotheses, because simply in the statements the researchers state in the conclusions that the hypotheses are verified, and in the presentation of the results of the research there is absolutely no argumentation. It is important to note, as Basic M. points out, "[...] Hypotheses are a tool that has the function of testing a theory, [...] therefore a hypothesis must be formulated in such a way that its verification is possible, and this is feasible only in a situation where its formulation expresses a theoretical predicament in accordance with the concrete social conditions of research ... it is necessary to transform the research question into a hypothesis that will be a guide in the process of research and which will thus help us to assess the adequacy of the theoretical explanation offered" (Besic, 2019).

Another element that should not be ignored, and concerns ethical issues. Bearing in mind that scientific research in the field of security often deals with sensitive topics, such as terrorism, crime, conflict and other types of violence, it can raise a number of ethical questions regarding the protection of the rights and personal data of research participants, as well as the correct interpretation and use of the research results. It is necessary to carefully consider the ethical aspects of research and ensure compliance with ethical guidelines.

It is inconceivable in modern conditions that scientific research is of an intradisciplinary character. Thus, security sciences, in their character, are an interdisciplinary field that encompasses various disciplines such as political science, sociology, law, psychology, military sciences, etc. This multidisciplinary approach can pose a challenge in terms of integrating different theoretical frameworks, research methods and data analysis. That is why it is essential for researchers to be familiar with different disciplines and able to integrate their approaches into research.

However, the above methodological problems are just some of the challenges that can be faced in designing scientific research in the sciences of safety. It is important to approach research with careful planning, the use of appropriate methods and continuous critical thinking to overcome these problems and provide valid and relevant research knowledge.

5. CONCLUSION

The methodology of scientific research is the basis for the successful conduct of scientific research. It provides the structure and guidance that researchers use to achieve research objectives in a systematic way. The subject and object of research methodology of security science refers to the study and understanding of the approaches, techniques, procedures and methods used in the analysis and research of the security field.

Designing research in the sciences of safety is a complex procedure that creates the necessary conditions for conducting research and obtaining relevant scientific knowledge and solving a specific scientific problem. The paper found that the sciences of security are interdisciplinary and that there is a direct link with military and political sciences. The methodology of security science is based on a multidisciplinary approach, combining elements from different

disciplines such as political science, sociology, psychology, law, informatics, statistics and other relevant fields.

It has been established that the research project, especially the part related to the scientific idea, is a key element for providing answers to questions concerning obtaining relevant scientific results and the preparation of doctoral dissertations. It can be noted that the research project essentially provides application to the scientific method and data analysis in order to gain a deeper insight into the nature of security and provide guidance for making relevant decisions in the field of security.

It was noted that in the sphere of designing research in the sciences of security there are certain methodological problems that are manifested most often in the form of: vague or avoidance of defining problem of research, problems of choice and selection of samples, validity and reliability and sample, omission or formal statement of verification of hypotheses, problems Ethical issues of data collection and interdisciplinarity and research.

REFERENCES

„Official Gazette of RS”, 114/2017 and 24/2020.

Besic, M. (2019). Methodology of social sciences. Novi Sad, ISBN 978-86-6263-280-7, Academic book.

Markovic, M. (1994). Philosophical foundations of science. Belgrade: BIGZ.

Mihailovic, D. (1999). Methodology of scientific research. Belgrade: Faculty of Organizational Sciences.

Milosavljevic, S. (1980). Research on political phenomena. Belgrade: Institute for Political Studies.

Milosevic, N. (1989). Designing Research in the Art of War. Belgrade: VINC.

Vujevic, M. (1983). Introduction to scientific work in the field of social science. Zagreb: Informator.

ASPECTS OF MACHINE LEARNING IN HUMANITARIAN DEMINING PROCESSES

Dejan Blagojevic^{1a}, Gordana Jovic², Aleksandar Milic^{3b}, Bojan Glamoclija⁴

¹ Academy of applied technical and preschool teacher studies Nis, Aleksandra Medvedeva
20, Nis, Republic of Serbia, dejan.blagojevic@akademijanis.edu.rs

² Academy of applied technical and preschool teacher studies Nis, Aleksandra Medvedeva
20, Nis, Republic of Serbia, gordana.jovic@akademijanis.edu.rs

³ University of Defence in Belgrade, Military Academy, Veljka Lukica-Kurjaka 33,
Belgrade, Republic of Serbia, aleksandar.milic@va.mod.gov.rs

⁴ Mine Action Center Serbia, Vojvode Toze 31, Belgrade, Republic of Serbia,
bojan.glamoclija@czrs.gov.rs

Received: 22th August 2023

Accepted: 28th August 2023

Review paper

Abstract: Machine learning algorithms require high-quality and diverse data to effectively train models. In the context of humanitarian demining, data collection includes gathering information regarding mine locations, types, soil conditions, environmental factors, and any other relevant variables. This data serves as the basis for developing machine learning models. Various machine learning algorithms can be applied in the context of mine detection, and the choice of the appropriate algorithm depends on factors such as the nature of the data, computing resources, and desired performance. Researchers and practitioners can experiment with different algorithms to find the most suitable one for their specific needs. This paper will present a review of some aspects of the application of machine learning elements in the analysis of terrain contaminated with explosives, with an emphasis on processing efficiency and a high degree of reliability of such an approach.

Key words: ERW, UXO, machine learning, algorithms, prediction

1. INTRODUCTION

Humanitarian demining is the process of clearing landmines and other explosive remnants of war (ERW) from areas affected by conflict. It is a dangerous and challenging task, but it is essential to the safety and well-being of civilians. Landmines and ERW are a major threat to civilians in many parts of the world (Mounu Prem at all, 2022). They can cause death, injury, and disability, and they can also prevent people from accessing essential services such as education and healthcare. Humanitarian demining helps to reduce this threat and to make it possible for people to live safely and freely. There are many different organizations involved in humanitarian demining. These organizations include governments, non-governmental

^a ORCID: 0000-0002-9086-4392

^b ORCID: 0000-0002-2642-0340

organizations (NGOs), and private companies. They use a variety of methods to clear landmines and ERW. One of them is manual demining. This is the process of clearing landmines and ERW by hand. It is the most dangerous method, but it is also the most effective. Another approach concern mechanical demining which presents the process of clearing landmines and ERW using machines. It is less dangerous than manual demining, but it is not as effective. Also, canine demining is presents and became innovative approach. Canine demining is the process of using dogs to detect landmines and ERW (P.A. Prada, M.C. Rodríguez, 2015). Landmines continue to kill and injure thousands of people each year, even decades after wars end. The vast majority of victims are civilians, including children. The removal of landmines is a slow and dangerous process, and it is often left to humanitarian organizations.

Humanitarian demining is a complex and challenging task, but it is essential to the safety and well-being of civilians. The organizations involved in humanitarian demining are working to make the world a safer place, one landmine at a time. There is numerous challenge we face in this process. The presence of landmines and ERW is often hidden from view. Landmines and ERW can be difficult to detect and remove. Despite these challenges, humanitarian demining is making progress. The number of landmines and ERW being cleared each year is increasing, and the number of people being killed or injured by landmines and ERW is decreasing (Hagenlocher et al., 2015).

Landmine detection poses numerous challenges due to the nature of these hidden explosive devices and the environments in which they are typically found (The Halo Trust 2011). Landmines come in different types, sizes, and configurations, making their detection more challenging. Some are made of metal, while others are made of plastic or composite materials, which can evade conventional detection techniques. Landmines are typically buried underground, making them difficult to detect visually. They can be concealed under soil, vegetation, or other camouflage materials, further complicating their detection. Many modern landmines are designed with reduced metal content or are completely non-metallic. This makes them difficult to detect using traditional metal detectors, which rely on detecting metal objects. The effectiveness of landmine detection can be affected by various environmental factors, such as soil type, moisture content, temperature, and vegetation density. These factors can influence the signals emitted by detection systems and cause false alarms or missed detections. Detection systems must be able to distinguish between landmines and harmless metallic objects commonly found in the ground, such as rocks or debris. High false alarm rates can lead to reduced efficiency and increased costs. Landmine detection technologies need to be affordable, portable, and suitable for use in various terrains and regions. This can be challenging, especially for developing countries affected by landmines, where resources may be limited. These operations involve inherent risks to the personnel performing the task (Knox, 2017). Ensuring the safety of operators and minimizing the risk of accidental detonation is of utmost importance. Finally, in areas affected by conflicts, landmines are often scattered randomly, making systematic clearance difficult. Inadequate records or maps of mined areas further complicate the clearance process.

Addressing these challenges requires the development of advanced technologies, including ground-penetrating radar, thermal imaging, acoustic sensors, chemical detection, and the use of drones and robotics. It also necessitates collaboration between governments, international organizations, and research institutions to enhance the effectiveness and efficiency of landmine detection methods.

There have been some attempts to develop new technologies to help with landmine clearance, but most of these projects have been unsuccessful. The humanitarian community still relies on outdated technologies, such as metal detectors and bayonets, to find and remove landmines.

There is a need for new and innovative technologies to help eliminate landmines. Multi-faceted demining machines, such as remote-controlled or semi-autonomous robots, could make the demining process safer and more efficient. These robots could eventually perform all of the major stages of landmine clearance, from preparing the ground to removing the mines themselves (Rafique at all, 2019).

In addition to demining machines, other technologies, such as unmanned aerial vehicles (UAVs), Ground penetrating radar (GPR) and advanced image classification and recognition software, can also be used to help find and remove landmines (Lameri at all, 2017). These technologies can be used to survey areas for landmines, identify likely mine locations, and even remove mines themselves (Liam at all., 2019). The development and deployment of new technologies to help eliminate landmines is a critical step in the fight against this deadly threat. By investing in these technologies, we can save lives and help communities rebuild after conflict.

Demining robots can be used to detect, remove, and destroy landmines. They are safer than humans and can work in more dangerous areas. Unmanned aerial vehicles are used to survey areas for landmines and to identify likely mine locations. They can also be used to deliver demining robots to remote areas. Advanced image classification and recognition software can be used to identify landmines in images and videos. This can be used to prioritize areas for clearance and to avoid unnecessary excavation. These are just a few examples of how new technologies can be used to eliminate landmines. As these technologies continue to develop, they will play an increasingly important role in the fight against this deadly threat.

2. MACHINE LEARNING CONCEPT

One of the major challenges in demining operations is the allocation of limited resources. The size of the area to be cleared is often much larger than the resources available. Additionally, the location of contaminated areas is often unknown, making it difficult to plan the deployment of resources effectively (Goodfellow at all, 2015). Currently, the allocation of demining resources mainly depends on non-technical surveys, demining dogs, and local knowledge. Non-technical surveys involve collecting information about the area to be cleared, such as its history of conflict and the type of terrain. One of powerful tool for solving these challenges is machine learning.

Machine learning is a subset of artificial intelligence (AI) that focuses on the development of algorithms and models that enable computers to learn from data and make predictions or decisions without being explicitly programmed. It involves teaching machines to improve their performance on a task as they are exposed to more data. Machine learning is a powerful tool with applications across various industries, including healthcare, finance, transportation, and more. Its continuous development and integration with other technologies like big data and cloud computing open up new possibilities for innovation and problem-solving. However, it's important to approach machine learning projects with a clear understanding of the domain, data, and potential challenges to achieve successful outcomes.

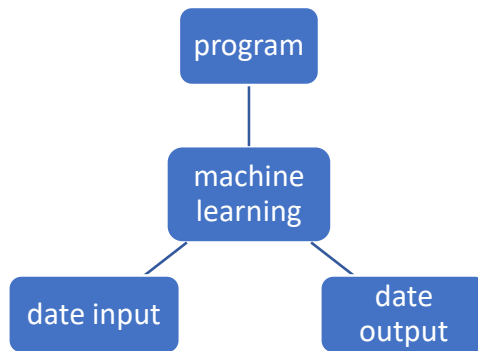


Figure 1. Concept of machine learning

Source: Authors

Machine learning algorithms use historical data as input to predict new output values. There are three main types of machines learning supervised learning, unsupervised learning and reinforcement learning. Supervised learning is a type of machine learning requires labeled data, which means that the output values are known. The algorithm learns to map the input data to the output values (Goodfellow at all, 2015). Unsupervised learning is type of machine learning does not require labeled data. The algorithm learns to identify patterns in the data without knowing the output values. Reinforcement learning presents type of machine learning that allows software applications to learn by trial and error. The algorithm is given a reward for taking actions that lead to desired outcomes and a penalty for taking actions that lead to undesired outcomes. Machine learning is a rapidly growing field with many potentials in humanitarian demining (Bajic & Potocnik, 2023). As the technology continues to develop, it is likely to have a major impact on our lives. Classical machine learning algorithms are often categorized by how they learn to become more accurate in their predictions.

3. RESULTS AND DISCUSSION

In first step, we try to create a date base of 3d models of mine used in this region in the past and now. In practice there are two main types of 3D scanners: contact scanners and non-contact scanners. Contact scanners use a physical probe to scan the surface of the object, while non-contact scanners use lasers or other sensors to scan the object without touching it. IN our case we used *Range vision smart 3D scanner*. For UXO in this case PMI mine, a non-contact scanner is typically used, as it is less likely to damage the UXO model. The scanner should be positioned so that it can capture all of the details of the UXO model. This may require moving the scanner around the UXO model or rotating the UXO model. For best results, the scanner should be positioned perpendicular to the surface of the UXO model. The number of points that are scanned will depend on the desired accuracy of the 3D model. For most applications, a few thousand points per square inch will be sufficient. However, for applications that require high accuracy, such as designing mine, a higher number of points may be needed.

There are a number of software programs that can be used to process 3D scan data. The specific software that we can use will depend on the type of 3D scanner that we have and the desired output of the processing. The 3D model should be inspected to ensure that it is accurate and complete. This can be done by comparing the 3D model to the actual type of mines. The mine should be clean and free of dirt and debris to ensure that the 3D scanner can capture accurate data. The scanner should be properly calibrated to ensure that the scan data is accurate. The scan data should be processed carefully to ensure that the 3D model is accurate and complete.



Figure 2. 3D model of PM 2 mine projection 2
Source: Authors

There are many different 3D modeling software programs available, each with its own strengths and weaknesses. Some popular options include Blender, Autodesk Maya, and SolidWorks, Scan center NG 2021. In our case we have used the last one.

After created the 3D models, we exported them into a format that can be imported into a database. Some common formats for 3D models include STL, OBJ, and FBX. We decided for, *.STL format. In next step 3D models in this format have been imported into a database, created by database management system (DBMS) MySQL. All models have been imported by DBMS's import tool.

After that, some of the standard set of algorithms for comparison between models and pictures could be applied. We can use a convolutional neural networks (CNNs) CNNs are a type of machine learning algorithm that are well-suited for image processing tasks. They can be used to extract features from images, such as edges, textures, and shapes. These features can then be used to compare the 3D model and the pictures.

In the case that UXO needs to be analysed through underlying structure of data, we can use autoencoders. This is a type of machine learning algorithm can be used to create a compressed representation of the 3D model and the pictures. This compressed representation can then be used to compare the two. Also, we are available to use generative adversarial networks (GANs) GANs are a type of machine learning algorithm that can be used to generate realistic images. They can be used to generate images of the 3D model and the pictures. These images can then be compared to each other to determine the similarities and differences between the two.



Figure 3. UXO, detected by UAV and H20T DJI camera
Source: Authors

The best method will depend on the specific application that we are using the comparison for. For example, if you are simply trying to see if the 3D model matches the pictures, then CNNs

may be sufficient. However, if we need to quantify the differences between the 3D model and the pictures, then we may need to use a more sophisticated method, such as autoencoders or GANs.

4. CONCLUSION

Currently, the allocation of demining resources mainly depends on non-technical surveys, demining dogs, and local knowledge. Non-technical surveys involve collecting information about the area to be cleared, such as its history of conflict and the type of terrain. Demining dogs are trained to detect landmines by their scent. Local knowledge can be used to identify areas that are likely to be contaminated. However, these methods are not always reliable. Non-technical surveys can be time-consuming and inaccurate, and demining dogs can be fooled by other objects that smell like landmines. Local knowledge can be outdated or inaccurate.

As a result, there is a need for more reliable methods for allocating demining resources. One promising approach is to use machine learning. Machine learning algorithms can be trained to identify contaminated areas based on historical data and other factors. This can help to improve the accuracy of the allocation of resources and make demining operations more efficient.

Machine learning can be used to identify patterns in historical data on landmine clearance. This data can be used to train machine learning algorithms to predict the likelihood of an area being contaminated. Also, machine learning can be used to analyze images and videos of an area to identify potential landmines. This can be done by identifying objects that are consistent with the appearance of landmines. Machine learning can be used to develop models of the behavior of landmines. This information can be used to predict where landmines are likely to be located. By using machine learning, it is possible to improve the accuracy of the allocation of demining resources and make demining operations more efficient. This can help to save lives and protect communities from the threat of landmines.

REFERENCES

- Mounu P., Miguel E. Purroy and Juan F. Vargas, (2022). "Landmines: the Local Effects of Demining", Toulouse, school of economics, https://www.tse-fr.eu/sites/default/files/TSE/documents/doc/wp/2022/wp_tse_1305.pdf
- P.A. Prada, M.C. Rodríguez, Demining Dogs in Colombia – A Review of Operational Challenges, Chemical Perspectives, and Practical Implications, *Sci. Justice* (2015), <http://dx.doi.org/10.1016/j.scijus.2016.03.002>
- M. Hagenlocher, et al., (2015), Spatial assessment of social vulnerability in the context of landmines and explosive remnants of war, *International Journal of Disaster Risk Reduction* (2015), <http://dx.doi.org/10.1016/j.ijdr.2015.11.003>
- The Halo Trust: HALO Utilizes Dual-sensor Detector | The HALO Trust (2011). <https://www.halotrust.org/media-centre/news/halo-utilises-dual-sensor-detector/>
- W. Rafique, D. Zheng, J. Barras, S. Joglekar and P. Kosmas (2019) "Predictive Analysis of Landmine Risk," in *IEEE Access*, vol. 7, doi: 10.1109/ACCESS.2019.2929677.
- Knox, M., Rundel, C., Collins, L.(2017). Sensor fusion for buried explosive threat detection for handheld data. *Detection and Sensing of Mines, Explosive Objects, and Obscured Targets XXII* 10182, May 2017. 101820D <https://doi.org/10.1117/12.2263013>
- Lameri, S., Lombardi, F., Bestagini, P., Lualdi, M., Tubaro, S. (2017). Landmine detection from GPR data using convolutional neural networks. In: *25th European Signal Processing Conference, EUSIPCO*, January, <https://doi.org/10.23919/EUSIPCO.2017.8081259>

Liam A. M., Wouter van Verre, Davidson J., Xianyang G., Podd F., Daniels D. and Peyton A., 2019. Combining electromagnetic spectroscopy and ground-penetrating radar for the detection of anti-personnel landmines. *Sensors* 19 (15).

Goodfellow, I., Bengio, Y., Courville, A. (2016). *Deep Learning*. MIT Press <http://www.deeplearningbook.org>

Bajic M., Potocnik B., (2023), UAV Thermal Imaging for Unexploded Ordnance Detection by Using Deep Learning, *Remote Sens.* <https://doi.org/10.3390/rs15040967>.

ENERGY SECURITY AT THE CORPORATE LEVEL

Radislav Jovicic¹

¹ Security Research Center, Street Sinise Mijatovica 9, Banja Luka, Republic of Srpska,
Bosnia and Herzegovina, radja21@hotmail.com

Received: 22th August 2023

Accepted: 29th August 2023

Review paper

Abstract: *Modern society, regardless of how aware we are of it, is completely dependent on energy, more precisely on access to sufficient amounts of energy. Today, it is impossible to imagine a modern man functioning for a single day without energy and energy sources - to come to work or university without means of transport; to stay or work in premises without heating, cooling and lighting; to store food and drinks; to carry out private or business communication; functioning of health and financial institutions. Disruptions in energy supply in the past, as well as the last one caused by the conflict in Ukraine, showed not only the great society dependence on energy and energy sources, but also the mutual connection and dependence of international subjects in the field of supply in order to ensure the necessary amount of energy sources. The availability of the required amount of energy, obtained from own or other sources, is the basis for the functioning of the state's economy, while the price of energy significantly affects the price of the final product and the competitiveness of the economy. Instability of energy supply at the corporate level can arise from various factors including geopolitical tensions, natural disasters, fluctuations in energy prices on the market.*

Key words: *energy security, corporation, energy, society, energy supplying*

1. INTRODUCTION

The term corporate security is related to the so-called the "epoch of corporate capitalism" where the state's economy was transformed from a system of companies that freely competed with each other into a system dominated by a relatively small number of large corporations owned by numerous shareholders. The second important determining factor of corporate security is that it is not binded to the state, sovereignty and territory, but to interest, necessity, feeling and identity as integrating characteristics of groups, societies and organizations. The main goal of corporate security is the security of business success accomplished by eliminating all risks and threats which can affect business activities and the achievement of business success, then reducing the threatening effects to the minimal possible extent and business functioning in crisis conditions, overcoming crises and normal dealings. Asymmetrical threats endanger the corporation's work and increase uncertainty in every business segment, particularly the security segment. The focus is being directed towards identification, evaluation and management of risk as well as implementing corporate security. Critical infrastructure is mostly seen in the energy sector. Facts that demonstrate that are:

- the majority of companies engaged in the production, transportation, processing or sale of energy sources are in most cases state-owned or majority state-owned;
- energy sources, the transition of energy sources or produced energy across the territory of an international entity, as well as the safe supply of energy in crisis situations are determined by national security policies;
- corporations of firms that are majority owners of individual sectors working with energy and energy sources have close coordination when it comes to security and defense measures as well as protection of energy and energy sources.

In view of the previously stated, one can sense the importance of energy and energy sources, that is, the importance of energy security for the stable functioning of society (in a sociological and political sense).

Defining energy security and recognizing its importance from the international subject level - state to the corporate level is the first and most important step in solving this issue. Regardless of the fact that energy security is no longer just an economic category and that energy products are often used as a means to achieve foreign policy goals, energy security has: infrastructure that needs to be identified and protected, sources of threats that need to be recognized and assessed, and the protection system and subjects that need to be organized, all of that in order to protect national interests, whether it concerns the state level or the interests that a corporation should achieve at its level without violating the national interests of the international subject, that is, the state.

There are many factors that affect the energy security of both countries and corporations: geographical location, size, natural resources, economy, politics, culture, technology and many others. Each factor individually and/or in relation to each other contributes positively or negatively to energy security. While some of the mentioned factors are constant (or difficult to change), others can be influenced by systemic approaches. For example, a change in policy can lead to binding to one source and/or supplier of energy sources, or influence the diversification of sources and directions of energy supply, in order to avoid economic dependence.

Dependence on one source and/or supplier of energy puts the corporation in a vulnerable position in the event of supply disruptions. Disruptions in supply can be caused by infrastructural difficulties and accidents, but they can also be caused by deliberate action, motivated politically, security-wise or economically. Suppliers who have a monopoly can use their position to obtain additional economic concessions from the corporation where they have a monopoly.

Asymmetric threats pose a risk for the work of the corporation and increase uncertainty in every business segment, especially in the security segment. Attention is increasingly focused on identifying, assessing and managing risks as well as implementing corporate security.

Through an analysis of available data sources in this field, this paper should, examine the position, significance, and role of energy security at the corporate level, and provide answers to some of the questions posed.

2. DEFINING THE CONCEPT OF ENERGY SECURITY

The phrase „energy security“ contains two concepts - energy (adjective: energetic) and security.

Energetics comes from the Greek word "ενεργεια" and implies a part of mechanics that studies the transmission and reversal of energy, that is, the economic utilization of available forces. From a philosophical standpoint, it is a view of the world where everything that exists and everything that happens is reduced to energy, which appears in different forms (Simic & Gostimirovic, 2017). In the economic sense, energy is "a set of economic activities by means of which primary sources of energy are explored and produced, then transformed, transmitted and distributed to consumers and rationally used as primary or secondary energy" (Djajic, 2011).

The term security comes from the Greek word "σφάλω", which means error, decay, defeat, or its negation "άσφαλο" which means secure. The second expression comes from the Latin "sine cura", and means the negation of trouble, that is, concern. From this basis, the English term "security" was derived, which means the feeling or state of freedom from threat. The concept of security in the Russian language is "безопасность" and means the absence of danger, protection from possible harm, and it is similar in French (*sécurité*), Italian (*sicurezza*) and German (*sicherheit*) (Simic, S & Gostimirovic, 2017). The military lexicon defines security as a state (protection of an asset, assets, society), organization (security services with appropriate capacities) and function (an inseparable attribute of the state regardless of the organization) (Ratkovic, 1981). According to aforementioned, "security generally implies the unhindered (unorganized and/or organized, planned and/or spontaneous) achievement, protection, development and enjoyment of reference values and interests, the absence of dangers that would call this into question (protection and harmlessness), and the absence of fear that it will happen (peace of mind, safety), as a product of predictability, certainty and organizational-functional abilities to control the development of phenomena that are constructive or destructive according to reference values and interests" (Mijalkovic, 2009).

According to one of the definitions, energy security includes a wide range of complex and diverse (geo)political, economic, security, military, and technological trends which is why it is often explained using compound or adaptable terms, with a focus on the words energy and security (*Bajagic, 2012*).

When defining the concept of energy security, it is necessary to address several key questions:

1. Whose security is being considered (the energy sector or the energy system);
2. What is security being considered for (the reference subject or object);
3. Security from whom/what (sources of threats to protected values);
4. Who will provide security (forces and resources) and
5. How will security be achieved (methods and activities) (*Simic & Gostimirovic, 2017*)?

Considering the aforementioned, countries view energy security from the perspective of an international subject. The United States, through its Homeland Security Act, places emphasis on critical infrastructure in its definition of energy security. The Energy Strategy of the Russian Federation contains a definition formulated as follows "energy security is the state of protection of the country, its citizens, society, state and economy by the safe supply of the required amounts of fuel and energy", i.e. "full and safe provision of energy resources to the population and the economy at affordable prices and, at the same time, stimulating energy savings, minimizing risks and eliminating threats to the country's energy reserves". The

European Commission defines energy security as the uninterrupted physical availability of energy resources in the market at prices that are affordable for all consumers (private and industrial).

The *Safety Culture* portal lists the four A's of energy security - Availability, Accessibility, Acceptability and Affordability (Safety Culture, August 21, 2023) as key elements of energy security. We find the mentioned elements or some of them in almost all definitions.



Figure 1. The 4 A's of Energy Security

Source: <https://safetyculture.com/topics/energy-security/>

Some authors believe that energy security appears as a subtype of ecological security, that is, by reducing the concept of energy security only to the availability of energy sources, stable deliveries in sufficient quantity and at acceptable prices, the definition narrows, and energy security is defined as a subtype of national security (Nadic, 2010).

For the purposes of this paper, we will utilize the definition that describes "energy security as a condition in which an international subject, the international community, or all its citizens have access to an adequate supply of energy at reasonable prices in the global market, free from challenges, risks, and threats that could result in disruptions in the supply of energy resources and energy" (Simic & Gostimirovic 2017).

3. DEPENDENCE OF THE CORPORATE LEVEL ON ENERGY SECURITY

The instability of energy supply at the corporate level represents a significant challenge for modern corporations. This instability can arise from a variety of factors, including geopolitical tensions, natural disasters, energy price fluctuations and supply chain disruptions. In order to identify energy challenges at the corporate level, corporations rely on research, analysis and expertise in the field of energy and energy supply.

In summary, the instability of energy supply represents a significant challenge for corporations. Identification of these challenges requires a multidisciplinary approach, which includes research in the field of energy, business strategy and geopolitics.

These are some of the key geopolitical factors and their impact on energy security:

Politics and legislation: The politics and legislation of countries can be key factors that affect the energy security of corporations. Changes in the political environment, such as the adoption

of new laws or changes in regulations, can have an impact on the stability of energy supply. For example, political decisions that limit the export or import of certain energy resources can create uncertainty and risk for corporations (Smith, 2022).

Geopolitical conflicts: Geopolitical conflicts and tensions between countries can lead to interruptions in energy supplies and threaten the energy security of corporations. Territorial disputes or political antagonisms can result in blocking or reducing the flow of energy through certain transit routes. Such conflicts can have long-term consequences for the energy stability and security of corporations (Johnson, 2019).

Energy diversification: Geopolitical factors may encourage corporations to develop energy diversification strategies to reduce the risk of political instability. Diversification of energy and supply sources helps corporations to free themselves from excessive dependence on certain regions or countries. In this way, the influence of geopolitical factors on the energy supply of corporations is reduced (Thompson, 2018).

Innovation and technological progress: Technological progress can have a significant impact on the energy security of corporations in the context of geopolitical factors. The development of new technologies for exploration, exploitation and renewable energy sources can reduce the dependence of corporations on politically unstable regions or resources (Davis, 2017).

International relations: Geopolitical factors are often reflected in international relations and cooperation between states. Agreements on energy cooperation, trade policies and diplomatic relations can affect the energy security of corporations. Openness to international cooperation and dialogue can help reduce the risk of geopolitical conflicts and maintain stability in energy supplies (Anderson, 2016).

Geopolitical factors have a significant impact on energy security at the corporate level. Politics and legislation, geopolitical conflicts, energy diversification, technological advances and international relations are all key factors that affect the ability of corporations to ensure a stable and reliable energy supply. Understanding and analyzing these factors are vital for corporations in order to identify risks and develop strategies for the protection and management of energy security.

Energy security has a key impact on corporate business, especially in the context of global energy challenges. First and foremost, energy security affects the business continuity of corporations. Energy supply is a key factor for carrying out basic operations, production, transport and distribution. Interruptions in energy supply, such as power outages or fuel shortages, can have serious business consequences. Energy security directly affects the financial sustainability of corporations. Energy price fluctuations, as well as political and geopolitical factors, can affect business costs. Increased energy prices or limited access to certain energy sources can increase operating costs and reduce profitability. Subsequently, energy security also has an environmental impact on corporate operations. With an increasing focus on sustainability and environmental protection, corporations are facing pressure to reduce greenhouse gas emissions and switch to renewable energy sources. Regulatory measures, as well as customer and investor demands for sustainable practices, influence the business strategies of corporations. This is precisely why business continuity, financial sustainability and environmental responsibility are key aspects that must be taken into account when managing energy security in the corporate sector.

Corporate business in the energy sector also faces certain risks, with the most significant ones being:

1) Financial risks and instability

Financial risks and instability represent a significant challenge for corporations in the context of energy security. These risks refer to possible losses or negative consequences that corporations may suffer due to fluctuations in energy prices, changes in the regulatory framework, geopolitical conflicts and other factors that affect energy supply. The management of financial risks and instabilities is becoming a key aspect of corporate business in light of the increasing challenges and complexities in the energy market.

Financial risks refer to the possibility of loss or negative impact on the financial results of corporations due to unpredictable changes in the energy market. Fluctuations in energy prices, which are often caused by changes in supply and demand, may have a significant impact on the profitability and competitiveness of corporations. As corporations often rely on energy as a key resource for their operations, sudden increases in energy prices can lead to increased costs and reduced margins, while sudden price drops can affect the revenue side and investment plans of corporations. Changes in the regulatory framework can also create financial risks for corporations. Government policies and legislation can have a direct impact on energy business, such as taxes, subsidies or regulatory requirements. Modifications in these areas may require significant adjustments to corporate strategies and investment plans. For example, the introduction of new regulatory requirements for reducing greenhouse gas emissions may require investment in new technologies or switching to renewable energy sources, which can be a financial challenge for corporations.

2) Operational risks and jeopardization of the corporate business sector

Operational risks are an important aspect of energy security at the corporate level. Corporations face various challenges that can threaten the continuity of their business. The key operational risks and their impact on energy security are: technical failures, natural disasters, instability of the political environment and cyber attacks.

Operational risks are an important aspect that affects the energy security of corporations. Technical failures, natural disasters, instability of the political environment and cyber attacks can cause interruptions in energy supply and put business continuity in jeopardy. To confront these risks, corporations need to implement effective risk management strategies and establish contingency plans. Also, diversification of energy and supply sources, monitoring of political trends and implementation of strong protection measures against cyber threats are key steps towards ensuring operational stability and business continuity.

The most serious threat to corporate sector security are crisis situations caused either by the manifestation of human activities, natural or artificially caused disasters. The preparedness of corporations to manage emergency situations is one of the fundamental elements for safe operation of a company or firm. The phases of preparedness for responding to crisis situations can be divided into: the preparedness phase, the response phase, the recovery phase, and the mitigation phase.

The preparedness phase refers to the activities that corporations carry out prior to an adverse event, thus enabling an effective response when an adverse event occurs. The basic characteristics of this phase are that a company engaged in energy and energy product-related businesses establishes basic procedures and plans for possible crisis situations, develops appropriate capacities and forces for reaction, and achieves coordination with all relevant entities that could provide assistance in specific conditions (local governments, state level, police forces, army and others).

The response phase in emergency situations consists of measures taken before, during and immediately after the end of the negative event. Response is the most difficult part of emergency management. By achieving a satisfactory level of preparedness, corporations reduce their own vulnerability and increase resilience to accidents. The reaction phase begins as soon as it becomes clear that a negative event is imminent and lasts until the negative event ends. After determining the real danger to the energy infrastructure, the management of the company tries to protect workers and facilities as much as possible by notifying the authorities at the local level. Exchange of information with local authorities and the measures and activities that are initially undertaken in energy facilities and plants can protect the local population and infrastructure, and provide: better organization of police and firefighting forces, deployment of human, material and technical resources, evacuation, rescue and emergency medical assistance. It is advisable that at this stage, if possible, the joint forces act as much as possible in accordance with the operational plans in order to approach the mitigation of the crisis and the transition to the recovery phase in a systematic way. The specificity of energy systems is that crisis situations can last extremely short, but the consequences can be catastrophic.

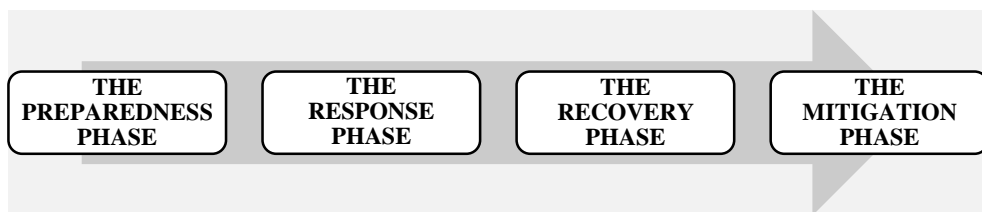


Figure 2. Phases of preparedness for responding to crisis situations
Source: Author's interpretation

The recovery phase is initially characterized by an unclear situation. Alongside the analysis and evaluation of damage caused by different types of emergency situations, priority repairs are also executed (parts of the energy production facility, possible installation malfunctions, information and communication system repairs etc.), demolition of damaged buildings, cleaning, waste removal and disposal, possible decontamination of the area, construction of new buildings, damaged infrastructure repairs, and such.

The mitigation phase, for companies in the field of energetics, involves efforts to remedy and mitigate the consequences caused by a crisis situation of any kind. When implementing mitigation measures and activities, it is crucial to also take into account natural, technical-technological, and social consequences of the emergency caused by the damage to the energy infrastructure. Certainly, the ultimate goal of mitigation should be resumption of continuous work.

When it comes to the attitude of corporations towards possible crises, five levels of their preparedness are mentioned: (Kesetovic & Kekovic, 2008).

- 1) Corporations prone to crisis (they do not have an early warning system, damage limitation plans rarely exist before a crisis occurs, and recovery systems are not yet in place);
- 2) Corporations that shy away from crisis (they often have programs for various types of disasters, but not for other types of crises, primarily external economic shocks or cyberattacks);
- 3) Corporations adapted to crisis (they have developed plans and procedures for a limited number of disruptions such as computer malfunctions, serious operator errors or major security breaches, but still do not understand the complex relations that contribute to the onset of crises);

4) Corporations strengthened by crisis (they do not represent progress in terms of types of crises they identify and in terms of implementing preventive actions, but have improved management of crisis phases - due to the establishment of proactive crisis management); and

5) Corporations prepared for crisis (have well-developed rules and procedures that explicitly take into account all critical systems that cause and prevent major crises, as well as a higher level of awareness about the existing organizational culture and its positive or negative impact on crisis management).

Every corporation should develop its own strategy for maintaining energy security because it is a key aspect of business. Considering multiple challenges that can affect the stability of energy supply, corporations must develop effective strategies to maintain energy security and minimize risks that could jeopardize their business continuity.

One of the most important strategies for maintaining energy security is the diversification of energy sources. Corporations should consider the possibilities of using multiple energy sources to reduce the risk of supply instability. This may include the use of different types of fuel, such as fossil fuels, renewable energy sources or nuclear energy. Diversification of energy sources provides corporations with greater flexibility and resilience to changes in the market or geopolitical factors that may affect supply.

Besides the diversifying of energy sources, corporations can implement an energy efficiency strategy. This strategy involves identifying and implementing measures that reduce energy consumption in operations. This can include the use of energy-efficient technologies, process optimization, or infrastructure improvements.

Energy efficiency helps corporations reduce their dependence on external energy sources and reduce operating costs. Another important strategy is the establishment of long-term energy supply contracts. Corporations can form partnerships with energy suppliers to ensure continuous supply. Long-term contracts provide predictability and stability in energy supply, reducing the risk of interruptions or fluctuations in energy prices. This strategy requires careful planning and market analysis to ensure adequate supply at favorable conditions.

Additionally, corporations can focus on developing internal capacities for energy production. This may include the construction of own energy facilities, such as solar or wind parks, hydroelectric or thermal power plants. This strategy allows corporations to be self-sufficient in terms of energy and reduce their dependence on external sources. It also provides an opportunity for corporations to generate additional income by selling the excess of produced energy on the market (International Energy Agency, 2020).

In addition, corporations can implement an energy storage strategy. The development and implementation of storage technologies allow corporations to accumulate the excess energy during periods when it is available and use it when demand is higher or when supply is uncertain. This reduces the risk of supply interruptions and provides corporations with greater flexibility in energy use.

Maintaining energy security is a key challenge for corporations that depend on energy for their business operations. Implementing effective strategies can help corporations minimize risks and ensure stability in energy supply. Diversification of energy sources, energy efficiency, long-term supply contracts, development of internal capacity for energy production and energy storage are just some of the strategies that corporations can enforce. It is important that corporations carefully analyze their needs, monitor market trends and develop customized strategies that match their specific business conditions (United Nations Development Programme).

4. CONCLUSION

Consideration of energy security at the corporate level reveals the importance of this issue for maintaining the stability and successful operation of organizations. In the modern world, corporations are exposed to various risks related to energy supply and must develop strategies that will allow them to effectively manage these risks. Alternative energy sources, renewable energy sources and improvement of energy infrastructure are key factors in ensuring energy security at the corporate level. Diversification of energy sources allows corporations to reduce the risk of energy supply instability, increase energy efficiency and reduce energy costs. Supplying traditional energy sources with alternative sources, such as solar and wind energy, and investing in infrastructure that supports renewable energy sources are important strategies for improving energy security. Furthermore, corporations should invest in technological solutions that will enable better monitoring and management of energy consumption, as well as the optimization of energy processes.

Integrating business ethics into all aspects of energy security management is critical to maintaining corporate integrity and accountability. Adherence to moral values, transparency in business, compliance with regulations and concern for environmental protection are important principles that corporations should follow. Business ethics play a key role in building trust with stakeholders and preserving corporate reputation. Leadership in the management of energy security plays a key role in successful implementation of strategies and achievement of desired results. Corporations should have leaders who are visionaries, capable of identifying future trends and challenges in the field of energetics and making decisions that will improve energy security. Leaders should be empowered with knowledge about energy technologies, regulations and trends in order to successfully lead organizations towards achieving a sustainable energy business.

The engagement and support of all corporate employees are key to the successful implementation of energy strategies. Every individual in the organization should be aware of the importance of energy security and contribute to the achievement of the set goals. This can be achieved through education, motivation and involvement of employees in the decision-making process and implementation of energy projects.

It is also important to emphasize the value of cooperation with external partners and experts in the field of energy security. Through partnerships with energy suppliers, technology companies, and research institutions, corporations can exchange knowledge, experiences, and best practices to improve energy efficiency and reduce risks.

REFERENCES

- Bajagic, M. (2012). *International Security*. The Academy of Criminological and Police Studies, Belgrade.
- DJajic, N. (2011). *Energy in Serbia - Yesterday, Today, Tomorrow*. The Academy of Engineering Sciences of Serbia, Belgrade.
- Johnson, E. (2019). *Energy Security in the Context of Geopolitical Conflicts*. ABC Press.
- Smith, J. (2022). *Geopolitical Factors and Energy Security*. London.
- Kestovic, Z., & Kekovic, Z. (2008). *Crisis Management Systems*. Faculty of Security and Protection, Banja Luka.
- Anderson, M. (2016). *International Relations and Energy Security: A Comprehensive Analysis*. JKL Publications.

- Mijalkovic, S. (2009). National Security. The Academy of Criminalistic and Police Studies, Belgrade.
- Nadic, D. (2010). Essays on Political Ecology. Faculty of Political Science, University of Belgrade.
- Ratkovic, B. (1981). Military Lexicon. Military Publishing House, Belgrade.
- Thompson, R. (2018). Diversification Strategies for Enhancing Energy Security. Oxford.
- Davis, S. (2017). Technological Innovations and Their Impact on Energy Security. GHI Books.
- Simic, S., & Gostimirovic, L. (2017). Energy Security - Challenges, Risks, and Threats of the Modern Era. College of Business and Technical Education, Doboj.
- Safety Culture. (2023, August 17). Energy Security. Retrieved from <https://safetyculture.com/topics/energy-security/>
- International Energy Agency. (2023, August 22). World Energy Outlook 2020. Retrieved from <https://www.iea.org/reports/world-energy-outlook-2020>
- United Nations Development Programme. (2023, August 22). Sustainable Development Goals. Retrieved from <https://www.undp.org/sustainable-development-goals/>

STRATEGIC MANAGEMENT IN CBRN EVENTS: APPLICATION OF WORD ASSOCIATION TEST

Halil İbrahim Çiçekdağı^{1a}, Fatime Ökenek^{2b}, Yıldız Tosun^{3c}

¹ Provincial Directorate of Disaster and Emergency, Konya, Türkiye, cicekdagi@gmail.com

² Provincial Directorate of Disaster and Emergency, Konya, Türkiye, okenekf@gmail.com

³ Provincial Directorate of Disaster and Emergency, Konya, Türkiye,
yildiz.tosun@afad.gov.tr

Received: 17th August 2023

Accepted: 24th August 2023

Original scientific paper

Abstract: This research aims to determine the perceptions of units involved in Chemical, Biological, Radiological, and Nuclear (CBRN) incident response regarding the CBRN discipline. A qualitative research method was employed for this purpose. The data collection tool used in this study was the Free Word Association Test, and the data was analyzed through content analysis. Maxqda 2020 data analysis software was utilized to perform the data analyses, resulting in a total of 18,620 codes. The results of the association test were categorized into associated individuals and objects, past events, intervention and protection methods, modes and sources of dissemination, outcomes, and types. Subcategory codings were conducted for each category. It was observed that certain concepts were lacking, and an attempt was made to establish a mind map diagram within the scope of the study to present these concepts. The analysis results revealed that the participants' perceptions of CBRN were limited. Therefore, an attempt was made to create a mind map to strategically manage sensitive topics like CBRN and to address training, exercises, and awareness-raising efforts within this framework.

Key words: CBRN, vocabulary, association test, strategic management

1. INTRODUCTION

The strength of modern societies is the result of their military resources, strategic and fragile assets, and the resilience of civil society. In the event of any threat or possible war, what determines the fate of that society is how long the military forces will continue to exist. When a terrorist attack, major accident, natural disaster, armed conflict, or other combined threat occurs, it is essential to recover quickly. Nevertheless, it is very important to support government institutions and fulfill their duties in emergencies. In these situations, both military and non-military elements must be ready to defend. Civil resilience is the ability to withstand any attack individually or collectively (Can, 2022).

^a ORCID: 0000-0002-3535-0647

^b ORCID: 0000-0001-6728-7171

^c ORCID: 0000-0003-4393-1975

Disaster management requires tactical, strategic, and operational planning. Therefore, disaster management is a subject that not only one branch of science but also many different branches of science deal with and examine together. This affects all societies due to the diversity of the impact area of disasters. Therefore, a multilateral governance system is required for disaster management. A disaster can stop the development of especially developed countries. Any development initiative without a strategic disaster management plan can cause post-disaster damage. Therefore, disaster risk should be strategically evaluated and planned in all areas of sustainable development. Therefore, not only intervention but also development should be addressed in disaster management. Sustainable development approaches require strategic planning for disaster management (Korkin & Öztop, 2022).

To be ready for threats, what needs to be done beforehand and a recovery plan afterward must be determined. For this purpose, first of all, awareness should be raised at the micro level, and training and exercises should be organized. At the macro level, the state should identify its physical or sociological weaknesses and risks. The government should also cooperate with the private sector. Thus, when the threat is over, the system will be restored quickly.

According to the Global Risks Report of the World Economic Forum published in 2023, environmental and climate problems are among the top six risks that are expected to affect the world economy over the next 10 years (World Economic Forum, 2023). Environmental problems are at the root of many meteorological disasters and epidemics we face in today's world. The dense smoke covering the sky of London, the capital of England, emerged at the beginning of the second half of the twentieth century as a factor that first pointed to the problem of air pollution worldwide. After that, chemicals such as DDT, which are used to meet the increasing food demand more quickly, drew attention to chemical pollution. (Carson, 1962). Then, depletion of the ozone layer was observed in the south polar region, causing it to focus on today's biggest issue - climate change. Similarly, according to the 2023 analysis of the Circularity Gap Report, which aims to move away from resource dependence, the circular economy rate of our world has decreased to 7.2%. Before the pandemic, this rate was around 9 percent. These changes reveal that humanity is in danger (Circular Gap Report, 2023).

CBRN hazards have existed in every period of history, but today, as technology and industry progress, many situations that can lead to CBRN incidents have emerged. Terrorist attacks and the use of CBRN-focused weapons are the most frightening of these situations. Therefore, it is very important to be prepared for CBRN and to intervene effectively, as in other types of disasters (Ergin, 2022).

The issue of CBRN is gaining more and more importance both in the world and in our country. This is because recent CBRN events and the dangers of CBRN and the magnitude of the effects they will create are becoming more and more aware every day. The attack with sarin gas in the Japanese subway, the September 11 attacks in the USA, and the anthrax incident that followed brought the disaster scenarios to be updated and the need for awareness and preparedness to be on the agenda (Kellek et al., 2009).

2. CBRN AND STRATEGIC MANAGEMENT

By adopting a strategic management approach to shape the future of the organization, analyzing the current situation, and determining performance indicators, activities, and projects in line with the targets; A systematic cyclical process that monitors and evaluates results is strategic planning. Here, it is important to apply the concept of strategic management together with planning. Thus, plans turn into a functional area for the future. In strategic management, where you want to be in the future is expressed with the vision, and future actions are embodied by the mission (Öztop, 2007).

The main purpose of public organizations in today's world is to determine the strategies and methods that will provide the best service to society most effectively and efficiently, and thus reach the goals and objectives. This can only be achieved by having a long-term vision to adapt to these changes in a rapidly changing world, and by putting forward and implementing the necessary strategies with this long-term perspective. An organization that does not have a strategy is an organization that cannot see its way forward and whose direction is not clear. Daily routine work cannot create an appropriate and compatible goal (Nuck & Backoff, 2009).

Strategic management is a management function involved in making decisions about where an organization should go and what it should do. The strategic management process takes precedence over all other management functions. Strategic management decisions are formulated, implemented, and evaluated in a way that enables the organization to achieve its goals and objectives (Howe, 1993).

In the CBRN Glossary prepared by AFAD, the abbreviation of chemical, biological, radiological, and nuclear concepts refers to the concept of CBRN. CBRN hazards and risks, previously defined as NBC (Nuclear, Biological, Chemical) in the literature, the use of contaminated weapons containing these substances in acts of terrorism and sabotage, the uncontrolled escape of CBRN substances used as products or intermediates in industrial production, health sector, laboratories and scientific research or natural disasters, damage and leaks in facilities containing CBRN substances (AFAD, 2022).

3. APPLICATION WORK

3.1. Research Method

This research aims to determine the perceptions of the Police, Health, Fire Brigade, Environmental and Urbanism, AFAD, and other related units, which are responsible for responding to chemical, biological, radiological, and nuclear incidents, whose short name is CBRN, towards the "CBRN" discipline. For this purpose, the qualitative research method was used in the study. In this study, the Free Word Association Test was used as a data collection tool, and the data were analyzed through content analysis. The application time of the test was determined as 30 seconds for a keyword, a total of five minutes. According to the results of the word association test, only the frequencies of the correct connections made by the relevant persons were taken into account, without considering the wrong words, and knowledge maps were created by the researchers by grouping them from the highest to the lowest. The data were gathered through the Google form system, through the test in which 1,862 people participated in the first ten words associated with the CBRN discipline.

The data obtained were evaluated according to the content analysis, categorized, and presented together with the frequency tables. To perform data analysis, Maxqda 2020 data analysis program was used and a total of 18,620 codings were made. Association test results; The people and objects associated with the association were divided into categories as lived events, intervention and protection method, mode and source of spread, results, and types, and sub-category coding for each category was carried out. Code cloud, single case model, code theory model, and hierarchical code sub-code model are the models revealed in the study.

In this context, the questions sought to be answered in the research are as follows:

1. What is the perception of the discipline "CBRN" in the relevant sample?
2. With which keywords can CBRN Association be classified?
3. What kind of mind map is available for CBRN perception?

3.2. Results

The findings reached within the scope of the research have been tried to be explained in the following sections. Tables and figures were created in order according to the research questions and related explanations were made.

Table 1. Demographic distribution of test takers (*Source: Authors*)

Number of Analysis	
Total Number of Testers	1.862
Total Number of Given Words	18.620
Gender	
Male	1.705
Female	157
Age Groups	
20-30	622
31-40	685
41-50	427
51 and above	128

When Table 1 is examined, 1,862 people participated in the analysis, and it is seen that 1,705 people are mostly male and they are in the 31-40 age group.

Table 2. Main and sub-coding made (*Source: Authors*)

<i>N.</i>	<i>Level-1</i>	<i>Level-2</i>	<i>Level-3</i>	<i>Level-4</i>	<i>Level-5</i>	<i>Freque ncy</i>
						15069
1	FEMALE					157
2	MALE					1705
3	CBRN CONNOTATION					0
4	ASSOCIATE PERSONS AND OBJECTS					0
5			GENEVA PROTOCOL			1
6			ORANGE TRUCK			1
7			MARIE CURIE			1
8			ACTUAL EVENTS			3
9				PEPPER GAS		4
10				MERCURY		4
11				CARBON MONOXIDE POISONING		7
12				METHANE EXPLOSION		2
13				ANTHRAX		43
14				JUNKMAN		1
15				TANKER ACCIDENT		2
16				CHERNOBYL		25
17				NAGASAKI		15
18				SARINE		8
19				WORLD WAR		3
20				OIL POLLUTION		5
21				CYANIDE		2
22				PLAGUE		6

<i>N.</i>	<i>Level-1</i>	<i>Level-2</i>	<i>Level-3</i>	<i>Level-4</i>	<i>Level-5</i>	<i>Freque ncy</i>	
23				COVID-19		5	
24				HIROSHIMA		22	
25			HITLER			1	
26			RESPONSE AND PROTECTION METHOD				0
27			MEDICINE			20	
28			ATROPINE			2	
29			PROTECTIVE EQUIPMENT				0
30				FILTER		3	
31				DISINFECTION		6	
32				CLOTHES		58	
33				AIR TANK		6	
34				MASK		254	
35				GLOVE		5	
36			BLEACH			3	
37			CIVIL DEFENSE			516	
38			PRACTICE			9	
39			PRECAUTION			134	
40			SHELTER			74	
41			EDUCATION			174	
42			SIREN			41	
43			DECONTAMINATION			35	
44			MEASUREMENT			38	
45				DOSIMETER		1	
46				DIAGNOSIS		42	
47				DETECTION		59	
48			METHOD AND SOURCE OF DISTRIBUTION				0
49			MICROWAVE OVEN			2	
50			BASE STATION			3	
51			SPREY			1	
52			DUST			4	
53			DOMESTIC CHEMICAL				1
54			LEAK			31	
55			CONTACT			10	
56			FOG CLOUD			1	
57			AGENT			20	
58				FOSFOR		3	
59				URANIUM		30	
60				RAY		7	
61				GAMMA		2	
62				BETA		2	
63				ALFA		4	
64				VIRUS		26	
65				BACTERIUM		5	
66			WASTE			65	
67			BARREL			1	
68			RAPID			7	

<i>N.</i>	<i>Level-1</i>	<i>Level-2</i>	<i>Level-3</i>	<i>Level-4</i>	<i>Level-5</i>	<i>Freque ncy</i>
69			INDUSTRIAL FACILITY			44
70			WEAPON			437
71			ATTACK			331
72			TERRORISM			91
73			NUCLEAR POWER PLANT			92
74			ACCIDENT			88
75			EXPLOSION			187
76			POISON			157
77			EPIDEMIC			60
78			CONTAGIOUS			19
79			BOMB			127
80				ATOM BOMB		105
81		RESULTS				0
82			ECONOMIC RESULTS			13
83			ENVIRONMENTAL CONSEQUENCES			0
84				AGRICULTURAL LOSS		5
85				SPRAY		20
86				AGILE		65
87				PERMANENCE		7
88				ECOLOGICAL BALANCE		5
89			POLITICAL RESULTS			0
90				THREATENING		314
91				WAR		1204
92			EMOTIONAL RESULTS			0
93				ANXIETY		12
94				DEPRESSION		1
95				PANIC		13
96				SUSPICION		22
97				EERIE		1
98				MASSACRE		35
99				FEAR		72
100				FEELING OF INSUFFICIENCY		4
101				MAYHEM AND CHAOS		39
102				EXCITEMENT		2
103				OBSCURITY		1
104				RISK		43
105				FEELING OF DANGER		516
106				DISASTER		32
107			PHYSICAL RESULTS			0
108				CANCER		29
109				HERETICAL DISEASES		25
110					DISABIL ITY	34

N.	Level-1	Level-2	Level-3	Level-4	Level-5	Frequency
111				COMBUSTION		13
112				ILLNESS		140
113				RESPIRATORY DIFFICULTY		26
114				POISONING		33
115				DEATH		594
116		TYPES				0
117			BIOLOGICAL			1541
118			RADIOLOGICAL			1532
119			NUCLEAR			1456
120			CHEMICAL			1782

When Table 2 is examined, a total of 120 different main coding words were coded 15,069 times. In this context, it is seen that there are five different main code distributions. The main codes were divided into sub-codes up to four sub-levels and subjected to analysis.



Image 1. Code word cloud

Source: Authors

In Figure 1, it is seen that all codes coded by the MAXQDA (2020) program are created as linear scaled code clouds according to frequency numbers. This method provides a visualization opportunity for a better understanding of all encodings. In this context, it is seen that the most basic indicator that stands out in the coded words is the concept of Chemical, followed by the concepts of Biological, radiological, nuclear, and war.



Image 2. Single case model
Source: Authors

Within the scope of the single case model for all the words shown in Figure 2, some words are included according to the results obtained through the Maxqda program. When this is evaluated in terms of its visual importance, it is seen that the mind map of the whole work emerges from a single point of view. In this context, it is seen that the lines belonging to the concepts of chemical, male, biological, radiological, and nuclear are thicker.

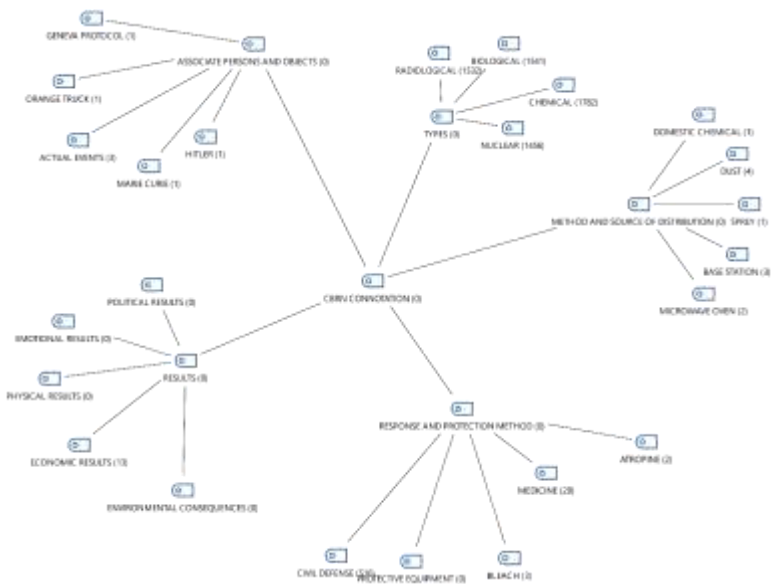


Image 3. Code Theory Model
Source: Authors

The Code-Theory Model shown in Figure 3 is similar in function to the Single Case Model. This model also focuses on a single code, but instead of displaying coded sections of code, it displays subscripts and notes. In the code map, the icon of the code is placed in the middle of the map with subcodes arranged in a circle around it. Subcodes can be arranged in two hierarchical levels, forming an inner circle around the first level code and an outer circle at the second level. Notes are linked to codes/subcodes with a line, and each code can be linked to several lines (Maxqda, 2022). In this context, figure 3 is the mind map of the study.

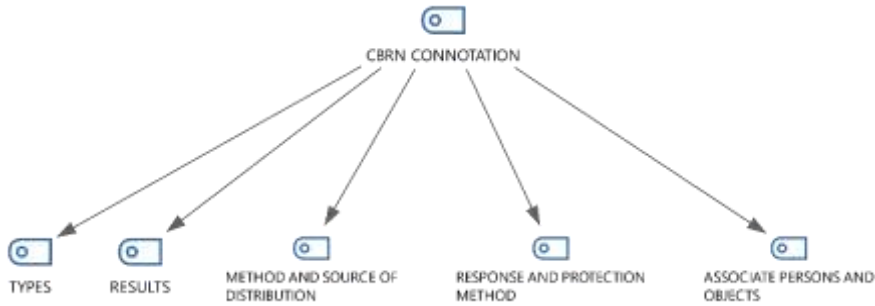


Image 4. Main Categories
Source: Authors

1. When Figure 4 is examined, the main categories of CBRN association are seen. These categories are; It is classified as type, result, mode, and source of spread, methods of intervention and protection, and people and objects associated with it.

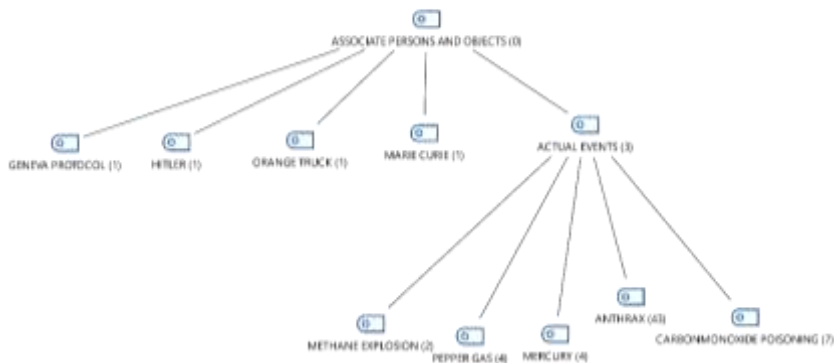


Image 5. Associated persons and objects
Source: Authors

When Figure 5 is examined, there are people and objects associated with it, which is one of the sub-categories of the CBRN association.

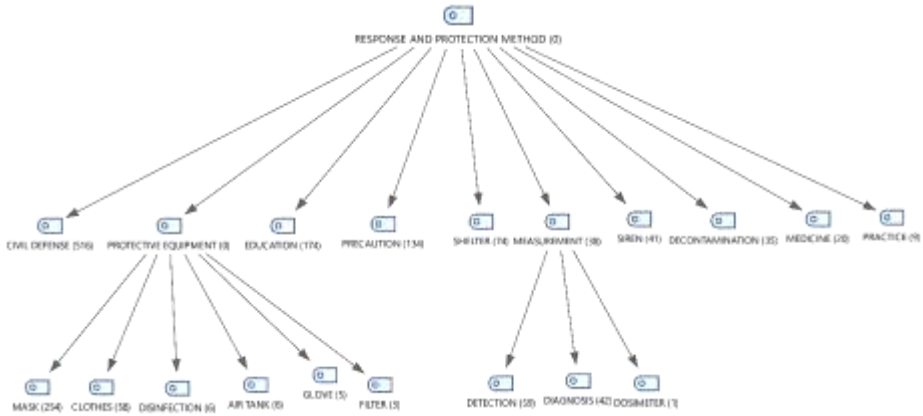


Image 6. Intervention and prevention method
Source: Authors

When Figure 6 is examined, intervention and prevention methods, which are one of the sub-categories of CBRN association, are included. The frequencies of all encodings are shown.

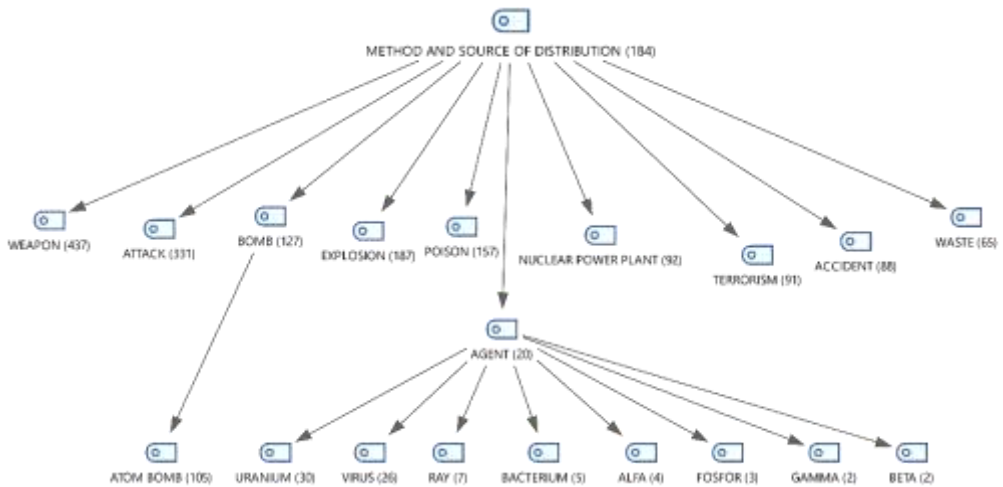


Image 7. Mode of spread and source
Source: Authors

2. When Figure 7 is examined, one of the sub-categories of CBRN connotation is its mode of spread and its source. The frequencies of all encodings are shown. It is seen that the codes in the form of weapons, attacks, and bombs have the highest frequency.

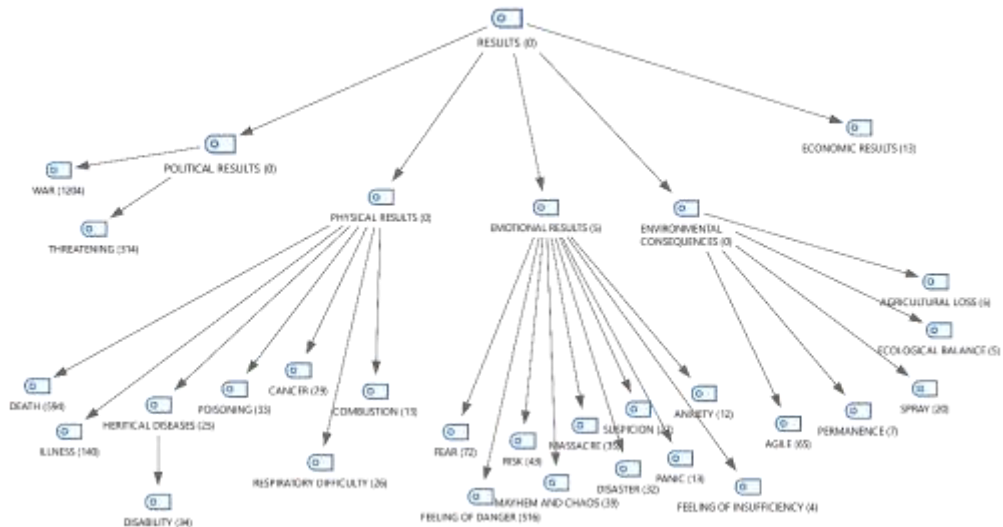


Image 8. Results

Source: Authors

When Figure 8 is examined, one of the sub-categories of CBRN association is found. The frequencies of all encodings are shown. These results are grouped under five categories: political, physical, emotional, environmental, and economic. While wars and threats are among the political consequences, some situations may arise such as death, illness, poisoning, and disability in the physical consequences part. Behind the emotional results, it is seen that the states of fear, anger, anxiety, and panic come to the fore.

4. CONCLUSION

When CBRN is considered strategically, the concepts of chemical, biological, radiological, and nuclear take place to a large extent as expected. The concepts that were seen to be missing and wanted to be gained were tried to be revealed by establishing a mind map scheme within the scope of the study. According to the results of the analysis, it was revealed that the perceptions of the people who participated in the test about "CBRN" were limited, and a mind map was tried to be drawn to strategically manage a sensitive subject such as CBRN and to deal with the training, exercises and awareness-raising activities to be carried out in this context.

While the urbanization brought about by industrialization in the world created a giant industrial society, it also highlighted individualism due to its contradictions and reduced compassion and solidarity within the society. Unprecedented in history, heavy and modern armament and industrial disasters also threaten humanity. The expectations of individuals before institutions and the state have reached the highest level in disaster situations with the contribution of social media. Thus, in this century of unnamed chaos, states and international organizations have accelerated efforts aimed at increasing their disaster preparedness capacity. In this study, CBRN events, which are man-made and can also be described as technological disasters in today's world, are evaluated from a strategic point of view.

When CBRN is considered strategically, the concepts of chemical, biological, radiological, and nuclear take place to a large extent as expected. The concepts that were seen to be missing and wanted to be gained were tried to be revealed by establishing a mind map scheme within the scope of the study. According to the results of the analysis, it was revealed that the

perceptions of the people who participated in the test about "CBRN" were limited, and a mind map was tried to be drawn to strategically manage a sensitive subject such as CBRN and to deal with the training, exercises and awareness-raising activities to be carried out in this context.

REFERENCES

AFAD. (2022). KBRN Sözlüğü. Afet ve Acil Durum Yönetimi Başkanlığı: <https://www.afad.gov.tr/tr/23793/KBRN-Sozlugu?kelime=kbrn> Accessed 01.07.2023

Can, A. (2022). Ulusal Güvenlik Açısından Kritik Altyapı ve Siber Alan: Sivil Hazırlıklılık ve Dirençlilik Perspektifinden Kavramsal Bir İnceleme. *Diplomasi ve Strateji Dergisi*, 3(2), 279-312.

Carson, R. (1962). *Sessiz Bahar*, <https://www.rachelcarson.org/>

Döngüsellik Açığı R. (2023). <https://www.circularity-gap.world/2023>

Dünya Ekonomik Forumu (2023), Küresel Riskler Raporu, https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf?_gl=1*nzo129*_up*MQ..&gclid=Cj0KCQjw756lBhDMARIsAEI0AgmAp6r-Ygtf4er-5rOnlZdh-jZs10bZcjXAPvPPG8cVjnUu0aL_0gwaAjyHEALw_wcB Accessed: 01.07.2023

Ergin, S. (2022). Hastanelerin kimyasal, biyolojik, radyolojik, nükleer tehdit ve tehlikelere karşı farkındalık ve hazırlık düzeylerine yönelik ölçek geliştirme çalışması, İstanbul Okan Üniversitesi, Lisansüstü Eğitim Enstitüsü, Sağlık Yönetimi Ana Bilim Dalı, Doktora Tezi

Howe, S. (1993). *Corporate Strategy*. Hongkong: The Mcmillan Press

Kollek, D., Welsford, M., and Wanger, K. (2009). Chemical, Biological, Radiological, And Nuclear Preparedness Training For Emergency Medical Services Providers. *Canadian Journal of Emergency Medicine*. 2009;11(4):337-42.

Korkin, E., and Öztöp., K., (2022). Büyükşehir Belediyeleri Stratejik Planlarında Afet Yönetimi. *Medeniyet Araştırmaları Dergisi*

MAXQDA, (2022). User Guide, Manual, Two-Cases Model. <https://www.maxqda.com/help.php?version=mx22&pdf=1&id=10011> Accessed: 01.06.2023.

Nutt, P. C., and Backoff, R. (1992). *Strategic Management of Public and Third Sector Organisations: A Handbook for Leaders*. Jossey-Bass, San Fransisco.

Öztöp, S. (2007). *Stratejik Planların Belediyelerde Uygulanması*, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi.

ENERGY SECURITY AS A PARADIGM OF CONTEMPORARY GEOPOLITICS

Srdjan Zgonjanin¹

¹ University of Defence in Belgrade, Veljka Lukica-Kurjaka 1, Belgrade, Republic of Serbia,
srdjanzgonjanin007@gmail.com

Received: 11th August 2023

Accepted: 21th August 2023

Professional paper

Abstract: *Why did energy and the narrative surrounding energy security take on almost manic dimensions in everyday life, so much so that this segment has become one of the most important vectors of the politics of every state and its „rulers”?*

This burning problem of today is the consequence, on the one hand, of the depletion of proven reserves of natural energy sources, and on the other hand, of the constant increase in the consumption of fuel and various types of energy in all segments of society. The energy picture of the modern world has noticeably become more complicated, both economically and politically. New powerful players with their own ambitions and long-term strategies have appeared in the energy markets. The fragile balance of power and interests in relations between energy exporting and importing countries, transnational energy companies and national states with strategic reserves of energy, energy producers and consumers is constantly changing...

Key words: *energy, energy security, geopolitics, resources*

1. INTRODUCTION

There are no easy or simple decisions, but we will have to act as soon as possible, otherwise we will face a disaster. The money that we will have to invest in our energy sector in the next 10, 15 or 20 years is between 16 and 33 billion euros.

President R. Serbia, Aleksandar Vucic (Vucic, 2022).

In recent years, with the increasing pressure of sanctions on Russia in various fields of activity, including the energy sector, the number of publications on various aspects of ensuring energy security has increased significantly. At the same time, the term "energy security" itself is often given too broad a meaning, including consideration of financial, foreign economic, environmental policy issues, etc.

Energy security, as a concept, appeared for the first time in the US National Security Strategy of Engagement and Expansion from 1996, within which a new chapter was dedicated to this area (A National Security Strategy of Engagement and Enlargement, 1996). After which this issue was inevitably described in all subsequent national strategies. After the mentioned American approach, the issue of energy security spread to the global level, which extended the general concept of security to the field of energy, which today occupies an indispensable part

of the consideration of national security formats, with an exceptional impact on the general security of any country.

Observing and studying the actions of the state as a subject of international relations in the sphere of economy and energy within it, we can clearly see that the race for resources, and especially for energy, has become increasingly dominant and that in the near future only the strongest and most proactive players will remain in it. The current crisis taking place in one of the most complicated hubs of the world, Ukraine, has fundamentally shaken not only Europe, but the entire world. The "turning of the taps" from energy sources by the countries with the richest natural resources has fully triggered the "butterfly effect", and the consequences of the swing of its wings have been felt by every individual, community, region.... The struggle for survival in the energy sphere is ongoing and she is crueler than ever....

2. WHAT IS ENERGY SECURITY TODAY?

In our country, the aforementioned change was first registered in the National Security Strategy in 2009, when it was recognized that security from the predominantly military sphere was extended to other areas, primarily economic, energy, social and environmental, including the security of the individual and society as a whole (National Security Strategy of the Republic of Serbia, 2009). In this context, our strategy then recognizes that "the ever-increasing definition of energy resources threatens the stability of individual countries and entire regions, as well as global security", while the geostrategic position of Southeast Europe, through which energy communication routes pass, connecting the developed countries of Europe with the regions of the Caucasus, the Caspian Basin, the Middle East and the Mediterranean, significantly and directly affects the state of security of the countries of the European continent (National Security Strategy of the Republic of Serbia, 2009).

Vincent Cable is among the first to define the place and role of energy within economic security (Cable, 1995). Namely, in 1995, he recognized economic security in the sense of the state's ability to unhindered acquire and produce resources that are necessary for the state's defense capabilities. There, in addition to trade in weapons and military equipment, he specifically described strategic minerals (cobalt, chromium, platinum, manganese), energy sources (oil and gas), food products, advanced technologies, etc. In addition, economic security can also be viewed through mechanisms of strategic economic influence such as sanctions and energy supply restrictions. A typical example of such a policy was found in the Middle East in the 80s of the last century, where the Gulf states, above all Saudi Arabia, used their dominant position within the Organization of Oil Producers (OPEC)¹ in order to influence American and other global and regional actors' policies. Namely, energy security became an international security problem as early as 1973, when the Arab oil embargo and the global oil shock occurred. The drastic increase in oil prices on the world market, caused by the Gulf War, dramatic indicators of global warming and depletion of non-renewable energy sources, as well as increasingly frequent crises due to the shortage of oil and gas, included the issue of energy security at the top of national security priorities (Bajagic, 2012). On the other hand, the suspension of Russian gas deliveries to Ukraine and Belarus in 2006 and 2007 can be taken as an example from recent history, while it is worth mentioning perhaps the most radical example in the last 15 years, when US Senator Richard Lugar² at one time even proposed the expansion of Article 5 of the Washington Treaty in the sense that the suspension of energy supplies against a NATO member state is also treated as an attack on the Alliance (Radoman, 2007).

¹ Organization of the Petroleum Exporting Countries - OPEC.

² Richard Green Lugar (Richard Green Lugar) was a senator of Indiana in the period from 1977 to 2013.

Furthermore, Susan Rice recognized poverty as the main economic threat to security, i.e. the weakening of state power (Rice, 2010), while the second one is the energy deficit, because without sufficient energy, states can experience economic, political and social collapse, and the absence of a reliable supply directly affects both external defense and the maintenance of a stable internal political and security environment. Hence the appearance of the classic definition of energy security, which refers to the availability of sufficient energy at acceptable prices. Daniel Yergin believes that security of supply, stability of delivery, availability at the most favorable prices, as well as physical security of gas and oil pipelines, are the default conditions for the security of most energy-dependent countries (Yergin, 2006). According to the aforementioned author, energy security includes the protection of the entire chain of energy production and supply, as well as the infrastructure used for these purposes. Yergin's theory has been extended by Jonathan Elkind, who considers four key elements in this area: (1) availability of energy sources and services, (2) protection of services from interruptions, (3) affordable and low-cost energy sources, and (4) environmental sustainability (Pascual & Elkind, 2010).

According to the Energy Strategy of the Russian Federation (RF) from 2003, "energy security is the state of protection of the country, its citizens, society, the state and the economy by the safe supply of the necessary amounts of fuel and energy", i.e. "full and safe provision of energy resources to the population and the economy at affordable prices and, at the same time, stimulating energy savings, reducing risks and eliminating threats to the country's energy reserves" (Bajagic, 2012).

Furthermore, Slobodan Simic defines energy security as a state in which an international entity or community, i.e. all its citizens, have access to sufficient amounts of energy at a reasonable price on the world market and without challenges, risks and threats that would lead to interruptions in the supply of energy and energy (Simic, 2017).

In the Republic of Serbia, the previously mentioned energy security provisions have been accepted, which is seen as a basic priority for the development of the country, achieving national and economic security, through maximizing independence from the import of energy sources and energy, with sufficient amounts of energy sources and energy, and in accordance with future energy needs (Ministry of Mining and Energy of the Republic of Serbia, 2022). However, our country considers separately the sub-term energy security, within which the necessity of a continuous supply of energy sources in various forms and in sufficient quantities, and at an acceptable price, is considered (Ministry of Mining and Energy of the Republic of Serbia, 2022).

3. EUROPE AND THE STRUGGLE FOR ENERGY SECURITY

No matter how you look at the relationship between geopolitics and energy security, it is important to note that the geopolitics of a country and its energy security are closely related (Bajagic, 2012). It can be explained in the following way - energy is a strategically important resource of every country, which is why they strive to gain control over its production, transportation, sale and consumption.

Global "geopolitics of energy" is, judging by the exact data of the International Energy Agency, which considers the scale of energy consumption at the global level, very present here. Namely, according to research by this institution, the USA and the EU (about 850 million inhabitants) annually consume 40% of the world's energy and energy sources, China about 20%, the RF and the post-Soviet space about 8%, Africa 4%, Latin America about 5%, while India and the rest of the planet, where about 40% of the population lives, spend only about 12% (Zdravkovic & Radosavljevic, 2022). The described scale of global energy consumption

shows the extent to which the energy crisis is affecting the European market, if it is taken into account that in the last two decades the USA made a breakthrough in the production of oil and gas from oil shale and became one of the largest global producers of energy.³

The energy crisis in Europe from the second half of 2021 has shown all the limitations of the West in its attempt to diversify energy supplies and reduce partial or complete dependence on oil and gas imports from the Russian Federation. Although numerous activities were previously undertaken in this direction, with the construction of the "Southern Gas Corridor" capital project and the opening of new terminals for the regasification of liquefied petroleum gas, the countries in the south, southeast and east of the continent still maintain a high percentage of Russian gas imports, which increases the potential for instrumentalization of the described situation by the Kremlin in terms of obtaining certain political concessions.⁴

In this context, the energy crisis showed that all European countries, except the Russian Federation and Norway, are to some extent dependent on the import of Russian gas. Moreover, in 2020 alone, the EU spent about 15 billion euros for the procurement of energy sources, while this amount increased to over 24 billion by the end of 2021. The same trend continued during 2022, where the war in Ukraine further intensified the energy crisis due to the reduction or complete interruption of supplies from the Russian Federation, the inability of Norwegian capacities to replace Russian gas and the insufficient export capacities of the USA, Africa and the Persian Gulf. Moreover, the events in Ukraine showed three key things: (1) that renewable energy sources, which the EU, led by Germany, insists on, they are not a reliable substitute for classic energy sources; (2) that political crises and especially the escalation of conflicts on the territory of Europe directly negatively affect the energy stability of all countries of the Old Continent; and perhaps one of the most important, (3) that the storage capacities even in the most developed European countries proved to be insufficient in cases of significant supply restrictions.

Until the beginning of the war in Ukraine, the Russian Federation was the leading supplier of energy for the European market. Unlike oil, which is mostly transported by sea, most of the gas is delivered via the pipeline network, which makes the mentioned system completely susceptible to market and political manipulations. Apart from oil and gas, RF is also one of the most important exporters of electricity, but this process is mainly oriented towards neighboring countries (post-Soviet space).

Moreover, while Europe, under the pressure of the USA, planned to diversify the supply of Russian energy products, the Russian Federation diversified its export routes towards Southeast and South Asia (if we consider the network of gas and oil pipelines towards the Indo-Pacific region).⁵ If we add to that the fact that the Asian market is far more attractive for large producers due to higher prices compared to Europe, but also a constant increase in

³ In 2019, the USA was the world's largest producer of natural gas with a total of 768.8 billion cubic meters of that energy, and the Russian Federation, the world's largest exporter of natural gas, fell to second place in the same year with 637 billion cubic meters of gas produced.

⁴ The above became most evident with the completion of the construction of the "Turkey Stream" and "North Stream 2" gas pipelines, which were accompanied by tensions due to bypassing the territory of Ukraine for the transport of Russian gas to the EU market and in our region.

⁵ It means the construction and completion of mega projects such as the Sakhalin - Vladivostok gas pipelines, the terminal in Vladivostok, the "Power of Siberia 1" gas pipeline, as well as the beginning of the construction of the "Power of Siberia 2" gas pipeline (the so-called Western route), which will cover through Mongolia China's complete natural gas needs.

demand due to positive demographic and economic trends in that part of the world. A similar strategy was applied in the case of oil exports. Namely, the Russian Federation is under sanctions due to the war in Ukraine and new conditions for the supply of oil to the European market.⁶diverted the accumulated surpluses of that energy source to India. Namely, with the new contracts with Moscow, this most populous country in the world received a long-term price discount of 20%, which brought the Russian Federation to the level of a strategic energy partnership in India and thus compensated for the losses caused by the interruption of supply to the European market.

Europe imports about 90% of its natural gas needs, of which, until the beginning of the Russian-Ukrainian conflict, about 41% came from the Russian Federation through the following gas pipelines: 1) three direct gas pipelines to Finland, Estonia and Latvia; 2) the Yamal Europe gas pipeline, via Belarus and Poland to Germany; as well as 3) five gas pipelines that ran through Ukraine to Slovakia, Romania, Hungary and Poland.⁷In addition to the above, from 2021, gas deliveries began via the "Nord Stream 1" gas pipeline across the Baltic Sea to Germany.⁸Furthermore, the new "Nord Stream 2" gas pipeline, despite the huge needs of the German economy and population for Russian gas, showed how much the political and geopolitical influence of its key opponents (USA, Ukraine and Poland) can affect energy flows in Europe.

Moreover, even Germany conditioned the commissioning of "Nord Stream 2",⁹while the sabotage of the gas pipeline, which led to its physical damage at the end of September 2022, pointed to the use of all available instruments of power by global and regional geopolitical actors in disrupting the energy dominance of one side.

Regarding the dependence on imports of crude oil and oil derivatives, the dependence of the European market reached its peak in 2019 when the EU imported about 98.8% of its needs,¹⁰of which the largest import was recorded from the RF (about 27%). However, despite the described indicators, the import of Russian oil has recorded a constant decline since 2005, when a record import level of about 18.7 million tons was recorded.¹¹The aforementioned decline is a consequence of the fact that oil imports are carried out via maritime waterways, as a result of which it was easier for the EU to find other sources of supply on the world market.

⁶ Moscow's decision not to sell oil to EU countries in dollars.

⁷ These are the following gas pipelines: 1) West Siberian or Trans-Siberian gas pipeline; 2) Gas pipeline "Brotherhood"; 3) "Predrak" gas pipeline; 4) "Savez" gas pipeline and gas transport route to Moldova, Romania and Bulgaria or the so-called The Trans-Balkan gas pipeline, which was deactivated in 2020.

⁸ The Nord Stream 1 gas pipeline is an investment by the Russian "Gazprom" (51%), i.e. companies from France, Germany and the Netherlands.

⁹ By delaying the implementation of the process of certification of the gas pipeline operator in the territory of the end user and making it conditional on the de-escalation of the conflict in Ukraine.

¹⁰ The import of crude oil and its derivatives in 2019 amounted to 507.2 million tons.

¹¹ Oil was transported by land to Europe via the world's largest oil pipeline "Friendship", which connects Russian Tatarstan with Ukraine, Belarus, Poland, Hungary, Slovakia, the Czech Republic and Germany.



Figure 1. Map of Russian gas export pipelines
Source: Author



Figure 2. "North Stream 2" gas pipeline
Source: Author

Faced with excessive energy dependence on Russian energy sources, the EU and the West began the reconstruction of the entire energy architecture of Europe, primarily through the construction of a new land and sea gas network, which included the construction of new floating terminals for the storage and regasification of liquid petroleum gas (LPG), mainly in the coast of the continent. The mentioned projects ensured the inflow of gas from deposits in the Caspian Sea, i.e. LPG from Qatar and the USA. The most significant European capital project is the construction of the so-called The Southern Gas Corridor for the transport of Azeri gas from the Caspian Sea, via Turkey, further to the south and southeast of Europe.

The Southern Gas Corridor consists of three major gas pipelines: 1) South Caucasus Gas Pipeline (from Azerbaijan to Turkey), 2) Trans-Anatolian Gas Pipeline (TANAP) through the territory of Turkey and 3) Trans-Adriatic Gas Pipeline (TAP) which transports gas through Greece, southern Albania and the Adriatic Sea to the south of Italy (picture 3). Thus, Turkey retained the role of the most important energy hub in Europe, through whose territory two gas pipelines from the Russian Federation and the Southern Gas Corridor cross. Thus, Ankara, seeing an opportunity to strengthen its own geopolitical position, along with the construction of capacity for the transport of Russian gas via the Turkish Stream gas pipeline (and partly Blue Stream), gradually increased the supply of American and Qatari LPG, i.e. Azeri gas from the Southern Gas Corridor. Although it retains slightly less than half of natural gas and LPG for the needs of its growing economy, in the manner described above, thanks primarily to its

geographical position, Turkey has profiled itself as a key gas giant from the point of view of Europe's energy security.



Figure 3. Supply of Southeastern and Central Europe with Russian and Azeri gas
Source: editing by author

Turkish Stream, which supplies the market of Southeast and Central Europe with Russian gas, was put into operation in January 2020, with the first deliveries of that energy to Bulgaria, North Macedonia and Greece, and later to Serbia, Hungary and Austria, i.e. to a lesser extent towards Bosnia and Herzegovina and Romania. Thus, the Russian Federation practically bypassed the territory of Ukraine, through which gas was delivered in the previous period via the so-called Trans-Balkan gas pipeline. In this way, Bulgaria, which, in addition to Turkey, is considered to be a low-profile Balkan gas hub, benefited from the mentioned projects, while in the future, Romania will also play a more significant role in the process of diversifying the supply of Russian gas, bearing in mind that the EU is helping to start the construction of a new regional the BRUA gas pipeline, which should connect important Black Sea gas deposits in the waters of Romania with Bulgaria, Hungary and Austria. In addition, the plan is to complete the reconstruction of the reversible flow of the Trans-Balkan gas pipeline (from south to north) in order to use its existing capacities for the transport of both Azeri and Black Sea gas from the direction of Bulgaria and Romania towards Moldova, which would make that country in the future could solve the issue of complete dependence on supplies from the Russian Federation, i.e. Ukraine.

In addition, the construction of another gas pipeline route from Bulgaria to Serbia (Novi Iskar - Dimitrovgrad - Nis) has also started, in order to enable our country from the direction of Greece and Bulgaria to also receive Azeri, as well as American/Qatar LPG (a new floating terminal in Constantinople). Brussels (with the support of the USA) is also helping additional projects in the Western Balkans in order to build new supply routes both from the direction of Greece and Albania (the project for the construction of the Adriatic-Ionian gas pipeline in the direction of Greece - Albania - Montenegro - Croatia with interconnectors to Bosnia and Herzegovina), as well and through the interconnector from Croatia (TNG terminal on the island of Krk).

The mentioned projects would essentially form an expanded network of the European Southern Gas Corridor, which would diversify the entire area of Southeastern Europe in the long term from the supply of Russian gas. If the route of the JANAF ("Adriatic Oil Pipeline") is added to the mentioned considerations, which is currently the only route to supply our country with this energy source, it can be concluded that the entire supply network of the Western Balkans will significantly reduce or completely ignore the need for Russian energy sources in the future.

4. CONCLUSION

It is a fact that at the global level "energy geopolitics" is today very pronounced and controlled to the greatest extent by the dominant energy powers - the USA and the Russian Federation, as a result of which the Russian-Ukrainian conflict, apart from the energy stability of Europe, had a significant negative impact on the energy safety and security R. Serbia. Thus, contrary to many years of efforts, European countries still do not have a fully diversified supply of the missing energy products, which creates space for the outbreak of new energy crises and disruptions in supply. In this context, certain countries of Central, Eastern and Southeastern Europe are more vulnerable in relation to the unstable energy market and security flows that occur in the West-East relationship, as a result of which they are naturally more susceptible to all the accompanying negative impacts that energy crises bring with them.

Although in the coming period the Russian Federation will continue to be, individually, Europe's largest supplier of energy, there is a need to regulate cooperation with Moscow in accordance with the uncertain political and security conditions of cooperation, while the USA will continue to press for a complete withdrawal from the aforementioned source. supply. However, the Western alternative is still insufficient in terms of supply sufficiency, with energy prices far less favorable than Russian natural gas and oil.

Positive examples of strategic thinking are visible in our immediate region. The completion of the "Southern Gas Corridor" and the continuation of the construction of the interconnector network in the Western Balkans represent a significant shift in the context of the diversification of sources and routes of supply. Also, a positive example is presented by Hungary and Bulgaria, which, regardless of the "security and energy umbrella" in which they are located, promptly started the construction of additional capacities for the storage of strategic gas reserves¹²and electricity, through capital investments in existing or construction of new blocks of nuclear power plants, which increased the aforementioned reserves many times over.

In addition to them, even the most developed European countries have recognized that it takes five to seven years, in principle until 2030, to get out of the energy crisis and ensure a continuous supply of energy (Zdravkovic & Radosavljevic, 2022). In this context, certain countries, such as Germany,¹³Turkey, France or Great Britain,¹⁴have temporarily given up on medium-term plans to shut down thermal and nuclear power plants and switch to renewable energy sources or gas processing technologies for electricity production. Moreover, 10 EU members led by France submitted an initiative to put nuclear energy on the "green energy" list (Zdravkovic, 2022), which represents another indicator of long-term strategic energy transition.

¹² Hungary, for example, today has storage capacities of six billion cubic meters of gas.

¹³ Germany planned to completely shut down 17 nuclear power plants with 22 reactors by 2026, in exchange for gas-fired thermal power plants.

¹⁴ Unlike Germany, France and Great Britain planned the construction of dozens of new so-called mini nuclear blocks for the production of electricity. Turkey, on the other hand, with the Russian "Rosatom" is building three nuclear power plants with four independent production reactors each, which will become operational in the period from 2023 to 2025.

REFERENCES

- A National Security Strategy of Engagement and Enlargement (1996). The White House
- Bajagic M. (2012). International Security, Criminal Police Academy, Belgrade.
- Cable, V. (1955). What is International Economic Security, International Affairs Vol.71, No.2
- National Security Strategy of the Republic of Serbia (2009).
- Pascual, C. Elkind J. (2010). Energy Security: Economics, Politics, Strategies and Implications, Brookings Institutions, Washington,-
- Radoman J. (2007). Energy securitization as an introduction to the energy security dilemma, Security of the Western Balkans, number 4
- Rice S. E, Graff C. Pascual C. (2010). Governing Poverty: Weak States and US National Security, The Brookings Institution, Washington.
- Simic S. (2017). Energy security - challenges, risks and threats of the modern age, Security Publishing Center, Doboj.
- Yergin D. (2006). Ensuring Energy Security, Foreign Affairs, Vol. 85, no.2
- Milos Zdravkovic and Goran Radosavljevic in the show 360 degrees (2022). available at https://www.youtube.com/watch?v=OcQM9a96_o0 .
- Milos Zdravkovic, "Because of bad management, we "ate" a thermal power plant", retrieved on November 21, 2022, from <https://milozdravkovicblog.wordpress.com/2021/12/16/zdravkovic-zbog-loseg-rukovodenja-pojeli-smo - one thermal power plant/>.
- Ministry of Mining and Energy of the Republic of Serbia, Energy Security of Serbia, 2022, <https://www.mre.gov.rs/aktuelnosti/saopstenja/energetska-bezbednost-srbije>.
- Vucic, A. (2022). Retrieved on November 20, 2022, from <https://24sedam.rs/biznis/finansije/176438/aleksandar-vucic-o-ulaganju-u-energetiku-i-obnovljive-izvore/vest> .
- Data collected during the visit of the 66th class of GSU to the NIS company, November 2022.

BEST PRACTICES IN CIVIL PROTECTION MANAGEMENT: IDENTIFYING CHALLENGES, RECOMMENDATIONS, AND INTERNATIONAL CASE STUDIES

Katarina Strbac^{1a}, Branislav Milosavljevic^{2b}

¹ School of Engineering Management, Vojvode Zivojina Misica 43, Belgrade, Republic of Serbia, katarina.strbac@fim.rs

² Faculty of Business Studies and Law, University of UNION Nikola Tesla, Jurijsa Gagarina 141a Belgrade, Republic of Serbia, banecuprija@gmail.com

Received: 13th July 2023

Accepted: 10th August 2023

Professional paper

Abstract: *Civil protection management is crucial in mitigating risks and ensuring effective emergency response. This article explores the identification and analysis of challenges and obstacles, provides recommendations for improving the civil protection management system, and presents international case studies showcasing best practices. By adopting a scientific approach, this article emphasises the importance of collaboration, continuous education and training, system evaluation, technological advancements, and interdisciplinary engagement. Through synthesising knowledge and practical experience, civil protection management can enhance its ability to protect communities, minimise damage, and promote resilience in the face of diverse challenges.*

Key words: *civil protection, management, resilience*

1. INTRODUCTION

Effective civil protection management requires an understanding of challenges and obstacles. By examining risk factors and vulnerabilities, stakeholders can develop innovative and efficient strategies to protect communities. The article presents an overview of best practices, focusing on risk assessment, continuous monitoring, multidisciplinary collaboration, and implementing preventive measures. The fact is that number of high-profile crises and disasters have driven the EU to increase cooperation among its member states in civil protection and to enhance its capacity to conduct civil protection operations in Europe and around the world. The EU's expanding role in civil protection mirrors its increased involvement in other security areas, such as fighting organised crime, combatting terrorism, and countering cyber threats. However, in the light of recent transboundary crises in the EU, manifested by the refugee crisis, terrorist attacks, and natural disasters, it is far from clear how effective such cooperative EU

^a ORCID: 0000-0001-7619-4639

^b ORCID: 0009-0009-1263-3108

arrangements can be due to differences in the way national civil protection has been organised and due to the question of whether sufficient trust exists within and between the involved organisations. (Parker et al., 2019) During the COVID-19 outbreak, it is evident that civil protection mechanisms play an essential role in protecting the population. For the first time in the history of humanity, the world encountered a global emergency that showed all the weaknesses of emergency management and the unwillingness of states to respond to that challenge adequately. (Strbac et al., 2022) After the outbreak, every country should reconsider the role of civil protection management in it.

2. IDENTIFICATION AND ANALYSIS OF CHALLENGES AND OBSTACLES

Comprehensive risk assessments are highlighted as a valuable practice, enabling the identification of potential threats and vulnerabilities. By involving experts from diverse fields, civil protection management can better understand the impact of these challenges on infrastructure, populations, and the environment. Additionally, establishing a system for continuous monitoring and analysis of information is emphasised, utilising advanced technologies for data collection and analysis. Engaging experts from various disciplines and fostering multidisciplinary cooperation is crucial for analysing complex problems and developing innovative solutions. Identifying and analysing challenges and obstacles in civil protection management is vital to understanding and effectively managing risks. Examples of good practice in this segment illustrate how these challenges are recognised and analysed innovatively and effectively. One example of good practice is the application of comprehensive risk assessments. In this case, civil protection management collaborates with experts from different fields to identify potential threats and vulnerabilities that may affect the community. Through detailed analysis, key challenges and obstacles are identified, as well as their potential impact on infrastructure, population, and environment. Another example of good practice is establishing a system for continuous monitoring and analysis of information. Civil protection management uses advanced technologies, such as sensors, data collection systems and analytical tools, to monitor relevant parameters and trends. This enables quick identification of new challenges and obstacles, as well as timely decision-making and taking of measures. Also, an example of good practice includes hiring experts from different disciplines. Civil protection management establishes cooperation with experts in technology, medicine, urban planning, sociology, and other relevant fields to understand challenges and obstacles better. Teams analyse complex problems together through a multidisciplinary approach and develop innovative solutions. (Indjic et al., 2013) Introducing preventive measures in response to identifying challenges and obstacles is also an example of good practice. Civil protection management recognises potential risks and actively takes steps to reduce their impact. Actions may include establishing early detection systems, educating the population, improving infrastructure, or implementing technological innovations. Through examples of good practice in identifying and analysing challenges and obstacles, civil protection management demonstrates the ability to approach complex situations systematically and efficiently. Through innovative approaches, multidisciplinary cooperation and the application of preventive measures, civil protection management ensures that the community is adequately prepared and resistant to various challenges.

3. RECOMMENDATIONS FOR THE IMPROVEMENT OF THE CIVIL PROTECTION MANAGEMENT SYSTEM

This section provides recommendations to enhance the efficiency and effectiveness of civil protection management systems. Establishing integrated mechanisms for cooperation and coordination among relevant actors is crucial, ensuring effective communication, information sharing, and joint planning. Continuous education and training for all stakeholders are vital to improving skills, knowledge, and emergency management capabilities. Regular evaluation and improvement of the system enable the identification of weaknesses and facilitate targeted enhancements. Strengthening technical infrastructure and technological capacities, such as advanced data collection systems and communication networks, are also recommended. Lastly, engaging experts and partners from diverse fields foster innovation and the development of advanced strategies and technologies for emergency response. Improving the civil protection management system requires careful consideration and application of appropriate recommendations to ensure the system's efficiency and effectiveness. Professional aspects highlight several critical recommendations for improving the civil protection management system. First, it is essential to establish integrated mechanisms for cooperation and coordination between all relevant actors. An integrated mechanism implies close cooperation between the government, local governments, civil protection management, the private sector, civil society, and other relevant institutions. Regular communication, information sharing, and joint planning are crucial for effective emergency response. (Dragisic, 2022) The second recommendation refers to continuous education and training of relevant actors. Civil protection management should provide regular training, exercises and simulations for all employees and associates to improve skills, knowledge and abilities related to emergency management. Also, educating citizens on how to act in emergencies and raising awareness of risks and preventive measures is essential. The third recommendation refers to the continuous assessment and improvement of the civil protection management system. Regular evaluations of the design, analysis of procedures during previous emergencies and feedback from relevant actors enable the identification of weaknesses and potential improvements. Based on these findings, civil protection management should improve plans, procedures, and capacities. (Indjic et al., 2013) The fourth recommendation refers to the strengthening of technical infrastructure and technological capabilities. Introducing advanced specialised tools, such as data collection systems, analytical software, sensors, and warning systems, can significantly improve emergency monitoring, identification and response. Also, improving infrastructure, such as communication systems, warehouses, and logistical support, enables a faster and more efficient response to crises. (Indjic et al., 2013) The last recommendation refers to the continuous engagement of experts and partners from different fields. Cooperation with scientific institutions, experts from various disciplines and partners from the private sector provides access to the latest knowledge, resources, and innovations in civil protection management. This cooperation can contribute to developing advanced strategies, techniques and technologies for protection and response to emergencies. Implementing these recommendations can significantly improve the civil protection management system and increase society's ability to face emergencies.

4. INTERNATIONAL CASE STUDIES

This section highlights international case studies that exemplify best practices in civil protection management. Italy's well-organised civil protection system, integration of different actors, and emphasis on training, exercises, and preventive measures are showcased. Norway's holistic approach, integration of all levels of government, and technological advancements contribute to its successful emergency management. Australia's comprehensive planning, use of advanced technology, community collaboration, and international cooperation are

highlighted. Japan's effective response to natural disasters, technological innovation, and cooperation with the population demonstrate its exemplary civil protection management system. The Netherlands' advanced flood warning system, infrastructure development, and stakeholder cooperation provide valuable insights into managing specific risks.

4.1. Italy

Italy stands out as an example of good practice in civil protection management. Their approach and experience in emergency management can serve as an inspiration and model for other countries. Italy has established a well-organised and coordinated civil protection system consisting of different levels of government, institutions, and organisations. In the Government of Italy, Minister for Civil Protection and Maritime Policy coordinates the relations between the government and Italian Civil Protection. At the national level, the Department for Civil Protection (Protezione Civile) has a crucial role in coordinating and managing emergencies. This agency is responsible for gathering information, analysing risks, planning and implementing preventive measures, and coordinating reactions in crises. (Allegretti, 2021) One of the critical features of the Italian system is its ability to integrate different actors and organisations in the decision-making and crisis management process. Strong cooperation exists between national, regional, and local authorities, the military, the police, health institutions, firefighters, the Red Cross and other civil protection organisations. This cooperation enables effective coordination of resources, information, and actions during emergencies. Italy also shows excellent attention in training, exercises, and simulations. Through regular training and exercises, civil protection management actors continuously improve their skills and prepare for different scenarios of emergencies. These activities provide an opportunity to test the system, identify deficiencies and improve efficiency in responding to crises. Italy also shows a strong commitment to preventive measures. In addition to a reactive approach, the country strongly focuses on identifying potential risks, planning and implementing measures to prevent them or reduce their consequences. This strategy reduces vulnerability and increases resilience to emergencies. An example of Italy's good practice can inspire other countries to improve their civil protection management systems. The Italian Department of Civil Protection (CP) encourages the participation of volunteer organisations in civil activities and emergency responses. They include psychosocial activities; social welfare activities, as assistance to the most vulnerable people (young people, the elderly, the sick, the disabled); the garrison of the territory; logistics and organisational support in case of natural or human-caused disasters, administrative and secretarial activities; prevention and an active fight against forest and interface fires; non-specialist site restoration activities and preparation and administration of meals; driving special vehicles; activities in the field of radio and telecommunications; diving activity; canine activities). More than one million people throughout Italy and more than 5000 organisations are registered on the National Civil Protection Department list (Roncone et al., 2021). Key lessons drawn from the Italian experience include strong cooperation between different actors, a focus on training and exercises, preventive measures and continuous system improvement based on identified deficiencies. These practices can help strengthen preparedness and manage crises in different countries more effectively.

4.2. Norway

Norway stands out as another example of good practice in civil protection management. Their holistic approach, high level of organisation and efficiency in responding to emergencies make them a model for other countries. One of the critical features of the Norwegian civil protection system is the integration of all levels of government, from national to local, as well as a wide range of relevant actors. The National Agency for Civil Protection (Directorate for Civil

Protection) coordinates and supports regional and local civil protection authorities. This agency provides guidance, training, and resources to ensure preparedness and effectiveness in responding to emergencies. (Morsut et al., 2020) Norway also has a well-developed preventive culture. The focus is identifying potential risks and implementing measures to prevent them or reduce their consequences. Preventive measures include clearly defined protocols and plans, regularly holding exercises and simulations, and intense supervision over critical sectors such as energy, telecommunications, transport, and health. Norway also shows high responsiveness and flexibility in responding to crises. Quick mobilisation of resources, good coordination between different sectors and effective communication are vital to their success. In addition, great attention is paid to psychosocial support for vulnerable communities, providing them with support and resources for post-disaster recovery. Norway also actively participates in international cooperation in the field of civil protection. Exchanging experiences, knowledge and resources with other countries contribute to global preparedness and efficiency in crisis management. Norway is an example of effective civil protection management that can be adapted to different scenarios and emergencies. Their holistic and comprehensive strategy, preventive measures, good organisation and quick response represent valuable lessons that can be applied in other countries to improve their civil protection management systems.

4.3. Australia

One additional example of good practice in civil protection management is Australia. Australia stands out for its comprehensive approach, advanced technology, and effective emergency management system. One of the critical features of the Australian system is a high degree of planning and preparation. The country has clearly defined protocols and plans for various disasters, including fires, floods, droughts, and other natural disasters. These plans include all levels of government and relevant actors and are regularly updated and PRACTICed to ensure efficient response to emergencies. Australia also uses advanced technology in civil defence management. It includes the Emergency Alert System, using drones for terrain monitoring and damage assessment, satellite monitoring of weather conditions and the spread of fires. These technological solutions enable faster decision-making, more accurate assessment of the situation and more efficient allocation of resources. An essential element of the Australian system is cooperation with the community. There is a strong focus on educating the population about disaster preparedness, evacuation, and self-protection. Local communities are encouraged to have contingency plans and participate in decision-making. It enables a faster and more efficient reaction in crises, with the support and engagement of the citizens themselves. Also, Australia is known for establishing international cooperation and exchanging experiences in civil protection management. Through international agreements, training and exercises, Australia contributes to global progress in emergency management and supports other countries in building their capacity. (Thomae, 2022) Australia's example of good practice highlights the importance of comprehensive planning, technological solutions, community collaboration and international cooperation in civil protection management. These practices can be an inspiration and model for other countries in improving their systems and increasing resilience to emergencies.

4.4. Japan

Another example of good practice in civil protection management is Japan. Japan is known for its practical approach to managing natural disasters, especially earthquakes, tsunamis, and typhoons. The Japanese civil protection management system is characterised by a high degree of planning, training, and technological innovation. The country has clearly defined disaster response procedures, which are integrated across all levels of government and sectors. These plans are regularly updated and rehearsed to ensure effectiveness in response. The Japanese

government also invests significant resources in the research and development of technologies that help predict and reduce the risk of natural disasters. An example is developing an early warning system for earthquakes and tsunamis, which enables faster notification and evacuation of the population before the disaster strikes. An earthquake early warning (EEW) system is designed to detect an event, determine its parameters (hypocenter, magnitude, and origin time), and alert sites/areas where necessary actions should be taken before destructive seismic energy arrivals. At present, large-scale EEW systems are operational in several countries around the world. The most extensive nationwide EEW system has been operating in Japan since 2007 and could issue alerts broadly when the magnitude (Mw) 9 Tohoku-Oki earthquake hit in 2011. This technology is critical to reducing loss of life and property damage. An essential element of the Japanese system is strong cooperation between the government, the private sector and citizens. There is an awareness that disasters are a common challenge and that all actors need synchronised action. The government actively cooperates with local communities, providing support and training for self-help and post-disaster recovery. Also, there is a culture of solidarity and willingness to help others in difficult times. Japan also shares its knowledge and experience with other countries through international cooperation. Japan contributes to global preparedness and disaster risk reduction through information sharing, training and technical support (Ishiwatari, 2021).

4.5. Netherlands

The Netherlands is known for its long-standing fight against floods and a developed civil protection system that focuses on warning and protecting the population from this natural risk. One of the elements of this system is the flood warning system, which is based on advanced technological solutions and a vast network of sensors distributed along rivers and coasts. These sensors continuously monitor water levels and transmit real-time data to crisis management centres. Based on the collected data, the system automatically analyses potential flood threats and generates warning messages distributed to many users, including local authorities, residents, businesses, and the media. These messages are sent through various communication channels, including mobile applications, SMS, email, television, radio and social media. It enables quick and efficient notification of people about the possible risk of flooding and provides them with guidance on the necessary protection and evacuation measures (Iwamoto, 2022). In addition to warning systems, the Netherlands has invested significant efforts in flood protection infrastructure, such as dams, levees, canals and reservoirs. It also continuously improves the regular maintenance and inspection design to ensure these protective systems' reliability and efficiency. The Netherlands flood warning system is an excellent example of the synergy between advanced technologies, infrastructure and cooperation with the population. This system results from many years of experience and learning from past floods, enabling quick reaction and efficient emergency management. This good practice is often recognised as a model for other countries facing similar flood risks.

5. CONCLUSION

Civil protection management plays a crucial role in strengthening the resilience of communities and effective response to all emergencies including outbreaks. The involvement of civil society, cooperation with the government and local self-governments, partnership with the private sector, identification of challenges and obstacles, and recommendations for improving the civil protection management system are critical factors for successful risk management. The involvement of civil society in civil protection management enables the creation of sustainable partnerships, raising awareness of risks and preparing citizens for emergencies. Cooperation with the government and local governments ensures coordination and efficiency in responding to crises. Collaboration with the private sector brings the

resources, expertise, and technical capacity necessary for effective risk management. Identifying challenges and obstacles enables a better understanding of the weakness of the civil protection management system. Based on this, the system improvement recommendations offer guidelines for improving integrated mechanisms, education and training, system evaluation, technological infrastructure, and expert engagement. Civil protection management can effectively manage emergencies, minimise damage, and protect citizens' lives and property through these strategies and measures. Building resilient communities requires continuous work, cooperation and exchange of knowledge and experiences between all relevant actors. Only through joint efforts can we build a society ready to face the challenges and unpredictability of the future. Civil protection management has a crucial role in preserving the safety and well-being of the community. A systematic approach, inclusiveness and continuous improvement are the basic principles that will ensure the efficient functioning of the civil protection management system in facing the challenges of today's world. Only through the synergy of actors and best practices can we create a resilient society that can quickly and efficiently recover from emergencies and protect its citizens. By adopting scientific principles and implementing best practices, civil protection management can enhance its ability to anticipate, respond to, and recover from emergencies. Collaboration among stakeholders, continuous education and training, system evaluation, technological advancements, and interdisciplinary engagement are vital for success. Applying these practices and lessons learned from international case studies, civil protection management can effectively protect lives, reduce damage, and promote resilience in the face of diverse challenges.

REFERENCES

- Allegretti, U. (2021). Civil Protection: The Fight Against Earthquakes. In: Sorace, D., Ferrara, L., Piazza, I. (eds) *The Changing Administrative Law of an EU Member State*. Springer, Cham. https://doi.org/10.1007/978-3-030-50780-0_16
- Dragisic, Z. (2022). Mehanizam civilne zastite EU I Srbija . perspective saradnje. *Godisnjak Fakulteta bezbednosti*, (1), doi.org/10.5937/fb_godisnjak0-37881
- Indjic, D. Terzic, M. Ivankovic, N. (2013). Information systems in environmental risk management. *Vojnotehnicki glasnik*, 61(1).
- Ishiwatari, M. (2021). Institutional coordination of disaster management: Engaging national and local governments in Japan. *Natural Hazards Review*, 22 (1), 04020059. [doi.org/10.1061/\(ASCE\)NH.1527-6996.0000423](https://doi.org/10.1061/(ASCE)NH.1527-6996.0000423)
- Iwamoto, K. (2022). Port Modernization Perspective in the Netherlands and Japan: Highlighting the Contribution of Dutch Civil Engineers. *International Planning History Society Proceedings*, 19(1), doi.org/10.7480/iph.2022.1.6509
- Morsut, C. Kruke, B. (2020). Europeanisation of civil protection: the cases of Italy and Norway. *International Public Management Review*, 20(1)
- Parker, C., Persson, T. Widmalm, S. (2019), The effectiveness of national and EU-level civil protection systems: evidence from 17 member states, *Journal of European Public Policy*, Routledge, [doi10.1080/13501763.2018.1523219](https://doi.org/10.1080/13501763.2018.1523219)
- Roncione, R. Giusti, L. Mammarella, S. Salza, A. Bianchini, V. Lombardi, A. Prosperocco, M. Ursini, E. Scaletta, V. Casacchia, M. (2021). "Hang in There!": Mental Health in a Sample of the Italian Civil Protection Volunteers during the COVID-19 Health Emergency, *Int. J. Environ. Res. Public Health* 18, 8587. <https://doi.org/10.3390/ijerph18168587>

Strbac, K. Ilic, D. Milosavljevic, B. (2022). Public Health Management in The Republic of Serbia During the Covid-19 Pandemic, SECURITY FORUM 2022, 15th Annual International Scientific Conference, February 9th, 2022 at Matej Bel University in Banská Bystrica, Slovakia, Conference Proceedings, Banská Bystrica, Slovakia 2022, ISBN 978-80-973394-7

Tajima, F. Hayashida, T. (2018). Earthquake early warning: what does “seconds before a strong hit” mean?. *Prog Earth Planet Sci* 5, 63 <https://doi.org/10.1186/s40645-018-0221-6>

Thomae, D. (2022). The contribution of the Australian Defence Force to civil resilience. *United Service*, 73 (2), 7-9 <https://search.informit.org/doi/10.3316/informit.46838996392494>

MODERN ARMED CONFLICTS AND RESERVE MILITARY FORCES

Hatidza Berisa^{1a}, Goran Korsev²

¹ University of Defence in Belgrade, National Defense School, Veljka Lukica-Kurjaka
33, Belgrade, Republic of Serbia, hatidza.berisa@mod.gov.rs

² Doctoral student at the University of Defence in Belgrade, Veljka Lukica-Kurjaka
33, Belgrade, Republic of Serbia, goran.korsev@gmail.com

Received: 18th July 2023

Accepted: 16th August 2023

Review paper

Abstract: *Today, the world is faced with crises and conflicts which, due to the possibility of uncertain development, represent a real threat to global, regional and national security. New-old geopolitical rivalries and Cold War divisions have revived, even within the European Union itself. The development of the scientific-technological and informational factor enabled the networking of various state and non-state actors regardless of time and space distance. Modern conflicts require a more flexible approach with smaller, specialized units that can be quickly deployed to respond to changing situations, as crises and armed conflicts of a local nature are an increasingly frequent threat to security. Especially in this sense, the significant use of reserve military forces organized on the territorial principle, because reserve forces organized in this way do not lack the motive to fight both against regular armed forces of aggressors and against non-state actors and irregular forces.*

The authors point out that the modern operational environment is becoming increasingly complex, more dynamic in terms of duration and intensity, but regardless of the type, they represent a great challenge for the cooperation of the parties due to the operational weapons and the multitude of actors present in the area of operations. Therefore, the focus of the work is to point out that in modern wars, in addition to the regular forces, a very important role is played by the reserve military forces.

Key words: *defense, army, reserve, replenishment, mobilization*

1. INTRODUCTION

The obligations that citizens have towards the defense of the country they live in are certainly the most difficult duties that a citizen has towards the community, because no other obligation of a citizen towards the community requires the sacrifice of the highest values, such as life. The obligation to participate in the defense of the country is often confused with military obligation. The obligation to participate in the defense of the country is a complex duty, which, in addition to the military obligation, if it exists in a given country, includes a whole series of

^a ORCID: 0000-0002-9432-5273

other obligations, such as the provision of material resources for the needs of defense, the obligation to perform certain work tasks in favor of the defense of the country, the obligation to participate in protection and rescue organizations and actions, the obligation to train for the execution of defense tasks and many others. Therefore, military obligation is the most important, it is quite a complex obligation and includes a number of elements, but it is certainly not the only obligation citizens have towards defense (Dragisic, 2011). The organization of the armed forces of neighboring states, states that have opted for a military "neutral status" in international relations, and the armed forces of major powers is conditioned by the types and character of security challenges and threats, defense interests, necessary capabilities, and available defense resources.

The armed forces of the states are filled in a similar way, mostly by professional army, less by general military service, but all states rely on the reserve force. The army must have the ability to use the knowledge (military and civilian), skills and abilities possessed by the person in the reserve, to solve the timely selection and quickly fill the missing specialties, the ability to quickly integrate into the war structure, using selective filling and mobilization, and all in order to develop the ability to perform operational tasks. The latest conflicts in Ukraine, and before that in Syria, Iraq and Afghanistan show that the reserve military forces played a very important role. So it can be considered that the reserve military forces are actually permanent command units or temporary structures that are mainly filled with personnel assigned to the reserve. No matter how much technology advances and how much the physiognomy of modern warfare changes, one thing remains that wars are won precisely by those forces that have a good reserve composition at their disposal.

2. DEFINING EMERGENCY MILITARY FORCES

The concept of military reserves dates back to ancient times when soldiers were required to serve in the military during wartime but were allowed to return to their civilian lives during peacetime. In the course of the development of military thought and science, no consensus was reached, and no generally accepted definition of "reserve" was determined in the literature. So the interpretations are completely different and as a result there are inconsistencies in the definition of the basic categorical term, but the similarity and essential determination of that term from the military aspect is visible.

According to the lexicon of foreign words and expressions by Milan Vujaklija, the term reserve comes from the French word "reserve" which in general translation means "reserved right, fence, stock, reserve, what is left or what is kept in case of need". In the military sense, the meaning of reserves is that they are soldiers, non-commissioned officers and officers who have served their military service, i.e. completed a certain type and level of training, in a peacetime composition, and who are called up "under the flag" only in case of war (commencement and duration of combat operations). state of emergency (states of "imminent and war danger") (Vujaklija, 1980)

According to the dictionary of the Serbian language, "reserve" is a word of Latin origin and has several meanings, depending on the field of application: general meaning, in the military sense, in sports, in grammar and language. In the military sense, it means: a) the status of conscripts who have served their military service or whose active military service has ended and are invited to military exercises as needed, b) a part of the army that engages in combat as needed. (Dictionary of the Serbian language, 2007) According to the military lexicon, similar to the Lexicon of Foreign Words and Expressions by Milan Vujaklija, reserve is a word of French origin and means an element of battle order, combined tactical units, operational formations and strategic-operational groups. In defining the term military reserve, a clearer definition of the term is given it is "manpower and material resources that form one of the

bases of the war potential of a country or a coalition of countries, needed by the armed forces for life, work and armed struggle."

In the definition of the term military reserve, a more detailed definition of the term is given, that is "people and material resources that form one of the bases of the war potential of a country or a coalition of countries, needed by the armed forces for life, work and armed struggle." They represent a special category, so they are also called state war (military) reserves or national defense reserves, in contrast to commodity reserves that are used by the country's economy to wage war..." (Law on material and labor obligations).

3. CHARACTERISTICS OF MODERN ARMED CONFLICTS

The twentieth century, among other things, is characterized by an increasing number of non-traditional forms of conflict. This trend was particularly manifested in the period after the end of the Cold War, when there was an accelerated and, in scope and content, transformation of the conflict.

Modern armed conflict is a constantly evolving phenomenon that requires a flexible and adaptable approach to military operations. Acquiring experience means knowing the wars of the past and their physiognomy. Wars of the first generation (Napoleonic wars) were characterized by mass armies, while wars of the second generation (World War I) were characterized by mass armies, but firepower appeared as a dominant element. . The third generation war (World War II) is characterized by "blitzkrieg", i.e. a quick transition from one maneuver to the next. The fourth generation war (Vietnam, Iraq) is characterized by the "isolation of the battlefield", i.e. the "separation of the main defense forces from reinforcement and support forces, by fire strikes from land, sea and air, and the destruction of the armed forces by elements.

Fifth generation wars are characterized by the disorientation of the enemy. According to William Lind, although he calls it the "fourth generation" war (aggression against NATO in the FRY, armed forces in Syria, the Special Military Operation of Russia and Ukraine), it is characterized by a crisis of state legitimacy, i.e. the loss of the state's monopoly over war, primarily the loss of the loyalty of its citizens, the rise of non-state entities whose loyalty is governed by organizations-states-individuals who wage wars. These entities can be armed criminal, religious, ethnic groups within races, tribes and ideologies. (Lind, 1989) In the last two decades, 95 percent of armed conflicts happened within states, not between them. (Lind, 1989).

Modern armed conflicts are characterized by completely non-linear fighting methods that disorient the enemy and aim at his mental and moral-psychological paralysis. Their aim is to cause the collapse of the enemy from within, not to physically destroy his armed forces. The battlefield of fourth-generation wars does not only include the operational space of the armed forces, but includes more or less the entire society of the enemy.

By analyzing the experiences of modern conflicts from the recent past, we come to the unique conclusion that the state of the economy has been and will remain one of the main drivers of conflicts of various kinds. In modern asymmetric conflicts, the objectives of the participants are not limited to military objectives but include political, social, economic and even psychological aspects. In modern conflicts, they are a logical choice for terrorist groups and other asymmetric participants. The accelerated development and increasing use of information and communication technologies has significantly changed the modern world and the way conflicts are conducted.

Global trends in changing the contemporary environment will affect the sources, causes and ways of resolving conflicts. Applications of artificial intelligence, robots, coordinated and non-contact warfare and mass implementation of actions in the information and cyber dimensions will require the development of new, that is, the improvement of existing concepts of warfare. (www.gov.uk/government/publications/future-soldier-transforming-the-british-army).

In political theory, there are various theories that try to define and explain a political phenomenon or several political phenomena. When explaining war as a political phenomenon, it should be defined to a certain level of abstraction, as well as the determination of all relevant facts that rule in the social reality of the observed phenomenon. According to Dragan Simeunovic, the basic properties of political theory are: comprehensiveness, modernity and having value for contemporary research (Simeunovic, 2002). It is easy to conclude that contemporary armed conflicts are shaped by five key trends: long-range precision weaponry, unmanned and autonomous systems, increasing access to space, conflicts over access to space, conflicts in information space, and growing reliance on nuclear weapons and dual-use capabilities.

Based on the above, it can be concluded that the basic characteristics of modern armed conflicts are reflected in the following: Unpredictability of occurrence; the presence of a wide range of military forces and forces and assets that do not have a primary military purpose; improvement of the command system and transition from a linear command system to a network system; the increasing role of modern effective combat systems; simultaneous use of forces in all parts of the geographical space; the significance of the media and information on the course and outcome of the armed conflict.

It is very important that these characteristics retain their characteristics in modern armed conflicts, for the reason that practice shows us exactly how many the conflicts in Syria, Iraq, and even now with the military operation between Russia and Ukraine are being manipulated. Regardless of the past, present and future, there will always be dominant applications of characteristics in any format of combat.

4. THE USE OF RESERVE MILITARY FORCES IN MODERN ARMED CONFLICTS

Reserve military forces have a long history, and the concept of a citizen-soldier dates back to ancient Greece. Therefore, modern reserve military forces are organized differently and have different roles and functions. Today's reserve military forces are an integral part of the army and can be used in various ways, primarily in the defense of the homeland, as support for regular forces, and can be used in peacekeeping missions. With the change in the nature of modern conflicts, there is also a change in the concept of the use of military forces.

Reserve military forces make up more than half of the military strength of the armies of NATO member countries. The organization, composition, mission, training levels of reserve military forces generally vary within the Alliance. However, common characteristics for all military reserve forces are that they play an important role across the spectrum of national and NATO defense structures and in the event of a crisis they are required to perform tasks alongside regular forces.

Modern conflicts often strive for a more flexible approach; with smaller, specialized units that can be rapidly deployed to respond to changing situations, as crises and armed conflicts of a local nature become more frequent threats to security. Significant use of reserve military forces organized on the theoretical principle, because reserve forces organized in this way do not lack a motive to fight both against regular armed forces of aggressors and against non-state actors and irregular forces.

Examples from the past show us exactly how much the reserve military forces played a significant role in the defense of small countries against the aggressive acts of big powers, especially by using the experience of guerilla and partisan warfare. The war in Vietnam and the protest of the Afghan people against the USSR, and in the recent past, the USA.

An exemplary advantage of reserve military forces is precisely their ability to supplement the regular army in times of crisis or war. Such forces can provide additional forces to support active Army units, ensuring the smooth running of operations. By supplementing these units, the reserve force can ease the burden on regular military units, ensuring that they remain efficient and effective. Although there are challenges associated with the use of military reserves, careful planning and coordination can help overcome these challenges and ensure that military reserves are an effective and valuable asset to modern military operations.

Reserve military forces can be mobilized to provide additional support to law enforcement agencies and first responders during crises or natural disasters. This includes search and rescue operations, public order and medical assistance. And how the use of reserve military forces in the modern age can be useful in response to non-military challenges, risks and threats to the country's security.

In addition to the good side, there are also certain weaknesses or challenges of the reserve military forces. One of the primary challenges is maintaining readiness. For the reason that the reserve military forces mainly consist of individuals who have their regular civil obligations in citizenship, so there is also a responsibility towards their professions, which they deal with professionally. Also, a frequent challenge that appears is the problem of communication and coordination between regular and reserve units, especially in joint operations, or in operations when they are conducted with different compositions of units from different countries, mainly due to different procedures and protocols.

However, for certain challenges, a solution can always be found through improving communication and coordination between regular and reserve military units and through joint training and exercises, which will improve the building of trust and joint work.

In particular, to solve the problem of challenges, it is necessary to create adequate conditions for the reserve military to undergo regular training, and if necessary, additional training, with the aim of integrating with military operations. In the future, the use of reserve military forces is likely to become even more important in ensuring the success of military operations. As the nature of warfare continues to evolve, the military will acquire and exist in the flexibilities in which it finds itself, that is, the performance of its assigned tasks within military operations. From a modern point of view, potential aspects of the use of reserve formations in national security defense will always exist because the environment will change the course of combat and operations.

Almost all reserve military forces in the composition of any armed forces will tend to develop, together with regular forces, the necessary capabilities for use and achieving certain successes in armed operations. In addition to their traditional roles in national defense and security, military reserve forces will certainly contribute to intelligence gathering and cyber security operations. One direction is certainly the increased use of technology and automation to improve the capabilities of reserve units. It can be seen that drones and other autonomous systems can also be used to increase the capabilities of reserve units, as individuals with civilian expertise in these areas will be able to provide critical support and intelligence gathering in various military operations.

Another direction is reflected in the integration of reserve forces in cyber defense and cyber security. Cyber security is becoming an increasingly important part of national security and

defense, and reserve personnel with expertise in this area could be used to enhance the military's capabilities in this area. Which provides the opportunity to specialize for the proper use and inclusion of persons in the reserve composition?

5. THE EXPERIENCE OF USING RESERVE MILITARY FORCES IN MODERN CONFLICTS

The use of reserve military forces in US military operations in Afghanistan, Iraq and Syria was critical to the success of these campaigns. The US military reserve forces consist of soldiers who have civilian jobs, but serve in the army part-time, providing the US military with the necessary human resources, that is, strength and skills to carry out its missions. These forces are critical to sustaining unified ground operations. The U.S. Army Reserve provides the active military with operational capabilities and strategic depth to augment its collective capabilities.

Since 2001, the US Army Reserve has mobilized and deployed more than 300,000 troops to support operations in Iraq and Afghanistan, while providing approximately 15,000 troops to support missions around the world. (www.armypmil) The National Guard and Reserve provide more than half of the total capacity of the US Army. Although all components of the military share the same standards of training, doctrine and equipment, each is distinct, interdependent and intrinsic. It is planned to increase the reserve composition to 200,000, and the National Guard to 343,000 (www.armypmil). There are a number of important career fields in the Army Reserve, including civil affairs, medical, maintenance, religious service, military intelligence, military police and logistics support (Cancian, 2021).

Higher education is a key developmental step for reserve officers, and more than 34 percent have a higher education. The army as a whole is dominated by a high percentage of highly educated members of the reserve (about 75 percent are masters and doctors of science).

In Afghanistan, since the beginning of the operation called "Enduring Freedom 2021", the USA has mainly used reserve forces. Reserve soldiers are deployed in various roles including combat and logistical support as well as intelligence. According to the official website "Army Reserve" from September 2021, over 35,000 reserve soldiers have been mobilized in Afghanistan since 2021 (Wale et al., 2015) and provided key support to regular US forces in conducting operations (clearing road communications, providing medical support and conducting intelligence operations).

In Iraq, the Army Reserve played a vital role in operations called Iraqi Freedom and Inherent Resolve. In these operations, reserve military forces were deployed in different units, but they mainly performed tasks in combat and logistical support units, as well as military police units. According to the already mentioned website "Army reserve" from September 2021, these units provided support to the US forces in providing security for convoys, medical support and security and enforcement of the adversary. The military reserve forces also played a key role in the training of the Iraqi security forces, which was essential for promoting stability and security. (Wale et al., 2015)

In Syria, a reserve unit was deployed in support of Operation Inherent Resolve (Wale et al., 2015). Reservists are deployed in a variety of roles including intelligence, logistics and military police. Over 8,000 reserve soldiers have been mobilized in Syria. The Army Reserve has played an important role in the execution of US Army operations in Afghanistan, Iraq, and Syria. The Army Reserve has provided tremendous support to the US armed forces in various roles, in combat operations, logistics support operations, and intelligence operations.

In addition to the USA, which uses reserve military forces for its operations outside its territory, the Israeli armed forces are no less behind them. The Israel Defense Forces (IDF)

relies heavily on its army reserves. Reservists are citizens who have served their mandatory military service and are then called up to serve periodically throughout their lives.

6. CONCLUSION

The development and progress of society and the state largely depends on the ability to recognize and adapt to global trends. Threats, as well as opportunities, should be recognized, adapted to them, and accordingly find ways to realize one's own potential. Undoubtedly, there will be times when states will consider the interests that caused the conflict to be so important that they are willing to accept the costs of going to war. But the frequency of conflicts where a state sees its vital interests at stake and where war is seen as an acceptable means of promoting or protecting these interests is declining as the 21st century progresses. Regardless of the above, no matter how modern technology is, it can only come if it has human resources that are personified. In addition to the regular composition, the success of the war depends on the filling of the reserve composition, which requires training and competence.

The reserve composition of the defense forces of countries in the world essentially consists of military personnel who are not obliged to serve continuously full-time, except in the case of compulsory mobilization, which is usually reserved for the defense of the country.

The use of reserve military forces varies considerably between countries. In some countries, the mobilization and use of reserve military forces is limited to national defense. In others, it is available to respond to domestic natural disasters. It is widely recognized that an integrated, appropriately dedicated, motivated and ready reserve force provides a good strategic expansion opportunity for current military capabilities. Almost as important, the military reserve forces create a vital civil-military link between the regular forces and the civilian community at large, especially in the area of specialized skills that are difficult to develop in a military organization.

REFERENCES

Concian M. F. (2021). U.S. Military Forces in FY; Army, October 21. 2021, http://www.cis.org/analy-sis/us_military_forces-fy_2021-army

Dictionary of the Serbian language (2007)., Novi Sad, Matica Srpska

Dragisic, Z. (2011). The national security system of the Republic of Serbia. Belgrade: Faculty of Security

Law on Military (2009). Labor and Material Obligation, Official Gazette of the RS, no.88/09.

Ministry of Defense Future Soldier: Transforming the British Army, Govuk, November 25, 2021, (www.gov.uk/government/publications/future-soldier-transforming-the-british-army)

Wale P. Dari, R. E. Rohn, L. and Sollinger J. M. (2015). Operation Iraq, and FEDEEDO: Decisive War, Elusive Peace, Randcorporation

Simeunovic. D (2002) Theory of politics-rider, Nauka i drustvo, Belgrade.

Vujaklija, M. (1980). Lexicon of foreign words and expressions, Belgrade, Prosveta.

www.armypmil, The Multiple Dimensions of Talent in the Army Soldier", n.d utps://www.army/mil/article/20687)the-multiple-dimensions-of-talent-in-the-army-reserve- soldier.

SYSTEMATIC APPROACH TO RESOLVING CRISIS DUE TO EPIDEMIC/PANDEMIC DISEASES

Slobodan Simic¹

¹ Sector Security, M. Popovica 9, Banja Luka, Republic of Srpska, Bosnia and Herzegovina,
slobodansimicss@yahoo.com

Received: 21th July 2023

Accepted: 4th August 2023

Review paper

Abstract: *It is undeniable that threatened balances in the natural environment cause entropy in many segments of life on the planet. Lack and pollution of water, excessive exploitation and pollution of land, release or evaporation of chemical compounds into the constituents of the environment, inadequate monitoring of the environment influence the activation of pathogens in an indirect and immediate way. The method of their origin may be known, but they now appear in a modified form, there are different ways of transmitting them, their virulence has increased, and the human, plant and animal populations are not ready to recognize or quickly find an adequate solution to defend themselves.*

Analytical multi-criteria and multi-dimensional approach to the recently ended pandemic significantly determines cause-and-effect connections on efforts to act preventively on future pandemics from the point of view of various sciences and scientific disciplines, practical solutions, but also organizational segments and process functions of management.

The aim of the work is to determine the main areas that are considered in the planning, organization and implementation of activities on prevention, suppression of the spread and fight against epidemic/pandemic diseases, and to partially or fully form a system of dynamic modeling of the development of an epidemic/pandemic

Key words: *pathogens, epidemic/pandemic, dynamic modeling*

1. INTRODUCTION

Excessive exploitation of environmental constituents and changes and phenomena that appear as products led scientific and professional workers to look at the elements and segments that cause, encourage and spread epidemics/pandemics from different scientific platforms, levels of interactivity of different factors. It has been recorded that in addition to natural causes, which can be the melting of millennia-old ice surfaces above and below the sea surface, it can also be artificially created viruses and bacteria that can be fatal for human beings and plant and animal life.

Security paradigms, paradoxes and consequences now acquire new dimensions because already known security risks and threats now have an additional asymmetric effect.

If the health aspect itself is considered, then that narrower contextual plane gives an indirect and immediate reflection on health as a predominant point of view and on activities that arise from the medical aspect. When looking at the broader context, the imperative viewpoints and conception of sustainable development, the relationship between ecology and politics, socio-economic processes in general, but also contradictions in the pursuit of development projects.

The pandemic of the corona virus-SARS-CoV-2CV that causes the disease COVID-19 has had a devastating effect all over the world. As of May 20, 2020, 4,927,229 people have contracted the virus and about 324,035 have died from it. The Secretary General of the UN labeled it as a "threat to humanity". The dominant definition of the crisis that prevailed among executive politicians around the world is that the corona virus is extremely dangerous and that it should be fought by any means necessary. This led to draconian measures, literally closing down entire states, regions and municipalities (Christensen, Laegried, 2020).

2. ANALYTICAL APPROACH TO THE EPIDEMIC/PANDEMIC CRISIS

According to the development of science and scientific disciplines and from a sufficient time distance, the decomposition of the crisis situation caused by the corona virus pandemic can be carried out. The systemic approach enables not only an insight into the past situation, but also provides reflective effects on possible crises that would occur in the future.

Immediately after the end of the COVID-19 pandemic, Kevin M. Esvelt investigated the impact of this pandemic disease as well as the possibility that this and similar ones could be used to threaten security in the future. He set key premises that are reflected in the following: that not all viruses that could cause pandemics in the coming period are known; identification of this type of virus is when more than a thousand infected appear; one infected person can cause a pandemic reaction; viruses of this type can spread faster than the distribution of vaccines or drugs for this type of virus, and pandemic samples can be much more lethal than particles from nuclear devices and available to terrorists. Through his work, he emphasizes the importance of keeping viral samples, the modalities of their spread, and the fight against these forms of viruses. This work indicates how necessary it is to monitor various natural and social processes in order to act in a preventive manner in the fight against viruses (Esvelt, 2022:8).

During April 2023, a study by Austrian scientists who made an astonishing discovery - by analyzing the genes of microbes and discovered that thousands of previously unknown viruses "hide" inside their DNA, was published in the public. Scientists have found the DNA of more than 30,000 different viruses, embedded in the genes of various single-celled microbes, and the results of their research were published in the journal "Proceedings of the National Academy of Sciences". (Internet presentation: Dnevni avaz, May 2023). The study of viruses as the most numerous biological entity is now gaining even more importance.

In their work "Balancing the self", the authors Jackson and Moore (Jackson and Moore, 2022:3) point out that modern times are distinguished not only by conflicts, political turmoil, economic instability, but also by the difficult-to-achieve goals of good personal health and political stability.

Recognizing the inflammatory impact and consequences of the COVID-19 pandemic, a group of scientists, based on the direction of the US Congress, began researching the spectrum of the impact of this virus on international security and the living environment. The areas that are causally connected with the pandemic of this virus and on which fields it has the most impact have been established:

- World order, international institutions;
- The influence of the USA in the world;

- China's role as a potential world leader;
- US relations with Russia and China, including the pandemic as a tool for ideological confrontation;
- Relative predominance of democratic or authoritarian and autocratic regimes;
- Social tensions, reforms, transformations and stability in different countries;
- World economy, globalization and US trade policy;
- Characteristics of conflict management;
- Allies' defense budgets;
- Cohesion of the European Union;
- US national security budgeting;
- US defense strategy and military operations;
- US international aid programs and reduction of international debt;
- The amount of US attention devoted to international issues other than the topic of the pandemic;
- The role of the US Congress in setting and monitoring foreign and defense policy in pandemic conditions (Rourke, McInnis, Moodie, 2020).

All economic sectors and industries have been affected by disrupted global supply chains, weaker demand for imported goods and services, declining international tourism and declining business travel. Measures to combat the spread of the virus have particularly affected the SME sector and entrepreneurs. Unemployment and the number of people forced to seek state aid have increased dramatically. Many countries have "stepped out" of virus control measures to mitigate the impact of the economic crisis only to face the growing wave of cases in the fall of 2020, jeopardizing the recovery of the health system and further endangering human health. The exit strategy from the crisis was not linear, with possible strategies to stop and control the virus until the vaccine was available to a significant number of people (Jesic et al, 2021).

It is an interesting fact that despite the devastating impact of this virus, other, international aspects of security are also being investigated, on which most countries could not even have a declarative position during the pandemic.

3. A MULTIDIMENSIONAL RESPONSE TO AN EPIDEMIC/PANDEMIC CRISIS

An analytical approach to the outbreak, development, culmination and spread of an epidemic/pandemic indicates that cause-and-effect relationships arise from a combination of natural and artificial as well as socio-economic and technical factors. Given that the epidemic/pandemic is primarily a health problem, several factors are established from the point of view of the health system. According to the Manual of the World Health Organization (WHO, 2020) the discussion groups are divided into seven sections: prevention and health system preparation; communication during crisis situations and involvement of the social community; immunization; research and monitoring; organization of work of medical services for clusters and different cases; the need for special settings of the system and individual groups; public health and social protection measures. Accordingly, that pathogens are compatible in some cases, and in others not, the health platform for consideration should

contain assessments: the exact type of disease, approximately its exact outbreak, spread, mortality and the indirect impact of such a disease as a biohazard.



Figure 1a. Correlations observed during an epidemic/pandemic crisis provides a simple overview of problematic thematic units using a geometric figure with subsections as individual sectors. **Exhibit 1a:** Correlations observed during an epidemic/pandemic crisis
Source: editing by author

The other side of the rectangular parallelepiped considers the levels in the prevention and fight against the pandemic, which can be by taking individual and collective measures, that is, at the tactical, operational and strategic levels. As the basis of this segment, the division that can be followed in one international entity prevails and which as such uses the process management functions (planning, organizing, management, coordination and control) in solving the crisis situation caused by the pandemic. Furthermore, the next page of the square gives reflective effects on socio-economic relations, sociological approaches and relations apostrophized through factors: economy, politics, security, international law, religion, culture, ecological security, armed forces, technology, but also tradition and collective mentality as significant corrective factors of social reality. The interaction of the mentioned factors left traces on socio-economic processes, especially in times of crisis, when some of their effects multiply. Certain interactions between the mentioned factors always appeared in some form, recognizable for a certain era, transformed according to the historical moment. Undoubtedly, they leave an impact in a direct and indirect way during the outbreak, during and after the pandemic crisis.

On display 1b. a page that points to the need for humanity as a characteristic of humanity that should especially come to the fore during the loss of a large number of human lives stands out. The aforementioned features of global equality, solidarity, well-being, health care in agreement with the organizational elements of individual and collective care for the sick significantly indicate the need for empathy and humanity in its original form.

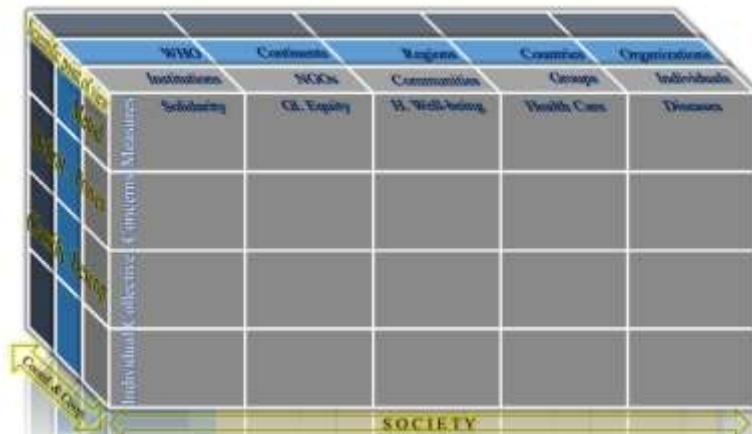


Figure 1a. Correlations observed during an epidemic/pandemic crisis provides a simple overview of problematic thematic units using a geometric figure with subsections as individual sectors. **Exhibit 1b:** Correlations observed during an epidemic/pandemic crisis
Source: editing by author

When the geographic-territorial approaches to the fight against COVID-19 are analyzed from this time distance, it can be seen that it was on a global scale and that organizations, associations and associations at that level, but also at lower levels, were compatible and synchronously fighting this honor using technical and technological achievements for the exchange and processing of data.

The world-wide crisis related to the COVID-19 virus has had catastrophic consequences for the economy and the population all over the world, and the importance of the response to this pandemic has been shown. All levels of government of the international subject - republican, provincial-regional, and local self-government authorities were faced with this pandemic (Karovic et al., 2021).

In order to coordinate activities from several scientific and practical areas, recommendations were given on the way of organization and operation of operational health centers in crisis situations, which were used in a certain way and with adaptation during the corona virus pandemic. The wider context in this publication gives an indication of how much care and support equipment must be taken to establish such a center at any level (WHO, 2015).

The scientific aspect of the analysis of epidemics/pandemics is multifaceted. This approach not only directs preventive activities in the field of natural sciences and medicine, but also provides a research path and procedures so that human lives can be saved or collectivities that are organized in different ways can be saved in a methodological way and with a proper approach in the fight against the pandemic.

4. CONCLUSION

It is evident and scientifically confirmed that epidemics/pandemics of a wider global scale occur periodically due to a number of causes. They are characterized by huge losses of human lives, disturbances in the socio-economic sphere, dysfunctions of social communities as well as entropy in the development of societies and states in general. An analytical approach to the epidemics/pandemics of various diseases recorded so far indicates that it is necessary to implement a systemic approach in order to provide an adequate response in a planned and organized manner in the coming period. The combination of looking at the cause-and-effect relationships about the emergence and spread of these wicked diseases indicates that it is

necessary to determine platforms (areas) that are compatible and whose optimal humanoid, scientific and technical-technological engagement can contribute to the reduction of crises caused by epidemic/pandemic diseases.

When the efforts of multi-criteria and multi-dimensional areas are sublimated, then the rules and restrictions in the field of social distancing, distance education, stricter controls in different spheres, disallowing the organization of mass gatherings and manifestations would have a more meaningful and purposeful character. It is also distinctive that the media campaign and the transmission of information through the media space have their own importance.

In the years to come, epidemics/pandemics of various types and characteristics can be expected with a high level of reliability, which can leave an impact on living beings and environmental constituents on the planet. Through a systematic analysis of previous epidemics/pandemics, it is necessary to apply the knowledge and lessons learned to the arrival of new ones, the same or even much more severe than the previous ones in terms of mortality. This is a necessity in order for our moral, spiritual and knowledge capital to pay off in huge dividends.

REFERENCES

A.O. (2023). Hiljade nepoznatih virusa skriveno u genima mikroba, Available from <https://www.avaz.ba/sci-tech/nauka/826104/hiljade-nepoznatih-virusa-skriveno-u-genima-mikroba>. Accessed 2023-05-01.

Christensen T. & Laegried P. (2020). The corona virus crisis-crisis communication, meaning-making and reputation management, In: *International Public Management Journal* 23-5.

Esvelt, M. K. (2022). Delay, Detect, Defend: Preparing for a Future in which Thousands Can Release New Pandemics, In: *Geneva Paper 29/22*, Geneva Center for Security Policy, Geneva.

Jackson M., and Moore M. D. (2022). *Balancing the self-Medicine, politics and the regulation of health in the twentieth century*, Manchester University Press, Manchester.

Jesic J. Andrejevic Panic A. Vukadinovic S. (2021). Managing local governments in a crisis caused by a pandemic in terms of economic survival and potential development, In: VII International scientific professional conference security and crisis management-theory and practice, Serbia, Belgrade.

Karovic S. Domazet S. Jesic J. (2021). *Lokalna samouprava u uslovima pandemijske krize*, Univerzitet Edukons, Sremska Kamenica.

Rourke, R., McInnis, K., Moodie, M., (2020). *COVID-19: Potential Implications for International Security Environment-Overview of Issues and Further Reading for Congress*, Congressional Research Service, Washington, DC.

World Health Organization (2015), *Framework for a Public Health Emergency*, Operations Centre, Switzerland, Geneva.

World Health Organization (2020), *Health system considerations: when influenza meets COVID-19 Preparedness and response measures when COVID-19, influenza and acute respiratory infections coincide in the WHO European Region*, Regional Office for Europe, Copenhagen.

RIVER BASIN WATER RETENTION CAPACITY COUPLING WITH NBS FOR HYDRO- METEOROLOGICAL DISASTER RISK REDUCTION

Branislava Matic¹

¹ Educons University, Faculty of Security Studies, Vojvode Putnika 87, Sremska Kamenica,
Republic of Serbia, branislava.matic@educons.edu.rs

Received: 5th August 2023

Accepted: 10th August 2023

Review paper

Abstract: *Sufficient water retention capacity contributes to hydro-meteorological risk reduction at the river basin level in many ways. The function and significance of the river basin water retention capacity for water management and DRR are manifold and documented in the literature. Accordingly, in the last few decades the interest to maintain or improve it is increasing, given the complexity of hydro-meteorological hazards and resulting risks. This paper presents an overview of two similar concepts based on improved ecosystem services: natural water retention measures and nature-based solutions from water management and disaster risk reduction perspectives. The similarities between the two concepts as hydrological ecosystem services are underlined, and indisputable benefits of the two concepts coupling for selected international river basin. Some open issues for better acceptance by practitioners are mentioned.*

Key words: *River basin water retention capacity, Nature-based Solutions, hydrological ecosystem services, river basin management, hydro-meteorological disaster risk reductions*

1. INTRODUCTION

Hydro-meteorological hazards are generated by natural processes and can not be prevented. They are complex events with diverse occurrences (frequency), time and spatial scale. In addition to devastating earthquakes, we are witnessing disasters resulting from hydrological, meteorological and climatological hazards globally. Comparison between the two periods (1980-1999 and 2000-2019) indicated disasters generated by natural hazards at the global level increased according to a report developed by (Centre for Research on the Epidemiology of Disasters- CRED & UN Office for Disaster Risk Reduction UNDRR, CRED&UNDRR, 2020).



Figure 1. Total disaster events by natural hazard type: 1980-1999 vs. 2000-2019
Source: CRED & UNDRR, 2019

Except for dry mass movement, significant expand in occurrence of disasters generated by natural hazards are evident in the second period as emphasized by Figure 1. For water-related events, the highest increase (74%) is observed for floods, followed by landslides (48%), storms (40%) and droughts (28%). Based on the report results, disaster impact increased in the latter period with respect to total death, affected people, reported total disaster number (75%) and economic losses (US\$) approximately 83%.

During the last few decades, there is growing interest in ecosystem services (ESS) and their contribution to hydro-meteorological hazard risk reduction. This generated number of concepts, approaches and definitions with respect to their ESS benefits while evidence-based capabilities from the perspective of natural features of the area and hydrology are sometimes neglected.

In recent years, Nature Based Solutions (NbS) concept is the most advocated as an all-inclusive innovative solution for the majority of issues that humanity is facing. Due to international policy processes and large amounts of funding pledged by both public and private entities, the number of NbS interventions is increasing exponentially (U. Nehren et al., 2023), the term NbS is being mainstreamed beyond expectations, for better and for worse, as it is subject to misuse and abuse, and has proponents and opponents.

Instead of detailed deliberation of the NbS concept advantages and disadvantages, this paper presents similarities with other ecosystem-based approaches the role of the river basin water retention capacity and its contribution to hydro-meteorological hazards Disaster Risk Reduction (DRR).

2. HYDRO-METEOROLOGICAL HAZARDS

Hydro-meteorological risks due to natural hazards such as severe floods, storm surges, landslides and droughts are causing impacts on different sectors of society (Ruangpan et al. 2020). They are unavoidable, with uncertainties regarding frequency and intensity, especially extremes (flood, drought, heavy rainfall) that are of particular interest for disaster risk reduction. The first step in their risk assessment is hydrologic (water) cycle components analysis.

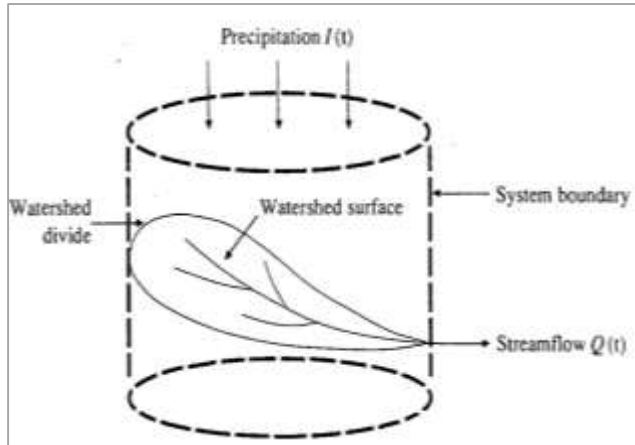


Figure 2. Simplified hydrological cycle terrestrial phase
Source: Chow et al., 1986

Either simplified water balance (Figure 2) or more complex depends on natural features and capacities of the hydrological unit (from small catchment to large river basins) to retain water. Runoff generation primarily depends on the intensity of precipitation and its time distribution. Due to the capacity of the river basin/ watershed/ catchment/ drainage area to retain precipitation the difference between the discontinuity of precipitation and the continuity of runoff is increasing (Jevdjevic, 1956) and a more uniform surface water runoff regime (quantity and speed) is generated. When the rainfall intensity exceeds the basin/catchment/drainage area water retention capacity, a series of events follows that lead to surface runoff (Srebreovic, 1986).

Hydro-meteorological hazards are integrated into water management planning documents. Alike DRR planning and management, water management is complex. To combat increasing pressures on water resources (water scarcity, pollution, climate changes, extreme hydrological events, land use changes, etc.) a new doctrine - Integrated Water Resources Management (IWRM) depicted in Figure 3 is incorporated in policy and legal frameworks at the national, transboundary, and global levels.

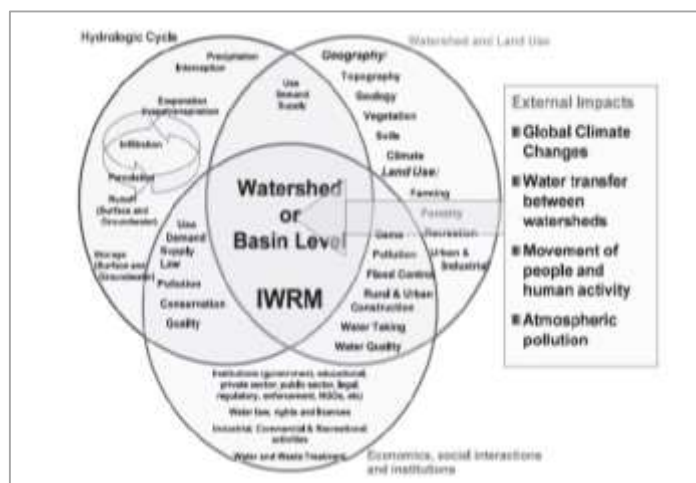


Figure 3. Conceptual IWRM integration
Source: Mayfield et al., 2004

IWRM attempts to integrate prospects and processes of the hydrologic cycle, watershed features and economics, social interactions, and policies (Mayfield et al., 2004) considering external impact with the main goal to address development, social equity, and environmental sustainability.

Natural hazards such as floods or storms can initiate events which challenge the safety and operation of hazardous facilities. Accidents triggered by such events are known as ‘Natech’ - Natural Hazards Triggering Technological Accidents. These impacts can also have a transboundary dimension (e.g., accidental pollution). The prerequisite for any DRR is to understand the risk which is not simple for hydro-meteorological hazards due to misunderstanding of drivers (frequency, intensity, land use and cover, and other boundary conditions).

EM-DAT classifies disasters based on hazards that generate them as presented in Figure 4 for hydro-meteorological and climatological events.

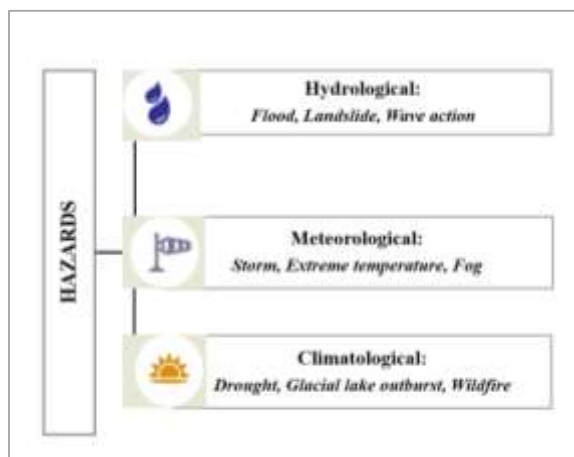


Figure 4. Selected disasters based on natural hazards type
Source: Developed by authors based on EM-DAT Guideline

To be included in EM -DAT disasters database an event must meet at least one criterion (ten or more people were reported killed, 100 or more people reported affected, declaration of a state of emergency, call for international assistance). At present, this is the most comprehensive database available worldwide.

3. HYDROLOGICAL ECOSYSTEM SERVICES AND WATER RETENTION FOR RISK REDUCTION: NWRM, NBS AND ECO-DRR

Hydrological ESS are water related and all ecosystems (terrestrial and aquatic) with a good level of service (not devastated) contribute more or less to hydro-meteorological and climatological hazards risks reduction by regulating runoff, infiltration, evapotranspiration, percolation, groundwater recharge, erosion processes, slope stability, etc. (Brauman et al.,2007). Water retention capacity is a hydrologic service that combines various ecosystems and their services. The most effective approach for water management is at the level of the river basin, sub-basin, and river district - the natural geographical and hydrological unit - instead of administrative or political boundaries. River basin district means the area of land and sea, made up of one or more neighbouring river basins together with their associated groundwaters and coastal waters, which is identified under EU Water Framework Directive Article 3(1) as the main unit for river basin management.

At the United Nations Environment Assembly (UNEA, 2022), governments formally agreed on a definition of nature-based solutions (**NbS**) as “actions to protect, conserve, restore, sustainably use and manage natural or modified terrestrial, freshwater, coastal and marine ecosystems, which address social, economic and environmental challenges effectively and adaptively, while simultaneously providing human well-being, ecosystem services and resilience and biodiversity benefits.” Ecosystem Disaster Risk Reduction (**Eco-DRR**) is the sustainable management, conservation and restoration of ecosystems to reduce disaster risk, with the aim to achieve sustainable and resilient development (Estrella and Saalismaa 2013). Natural Water Retention Measures (**NWRM**) are multi-functional measures that aim to protect water resources and address water-related challenges by restoring or maintaining ecosystems as well as natural features and characteristics of water bodies using natural means and processes. The main focus of applying NWRM is to enhance the retention capacity of aquifers, soil, and aquatic and water-dependent ecosystems, supports green infrastructure, improves the quantitative status of water bodies, reduces the vulnerability to floods and droughts and restore the natural functioning of ecosystems and the services they provide (EC DG ENV, 2016). Based on definitions for NbS, Eco-DRR and NWRM the difference is the terminology used to address ecosystem-based concepts with respect to water-related natural hazards. While NWRM efficiency and applicability have to be supported by hydrologic assessment and analyses, for NbS and Eco-DRR is not clear how the statement “measure (s) reduce risk” and contribute to DRR can be justified without request- hydrologic analyses. For spatial scale different terminology is used, landscape, area and natural geographical and hydrological unit for NbS, Eco DRR and NWRM.

Application of the NWRM at the transboundary Tisza River Basin supports environmental and flood risk management objectives synergy and integrated management (Matic et al., 2021). Both integrated river basin and DRR management planning are multidisciplinary, based on effective cross-sectoral cooperation, diverse stakeholders’ interactions, participatory approach, and update of plans. Different spatial dimensions for plans might be reconsidered to allow better maps, data and information overlapping for more effective DRR management, due to water-driven natural hazards nature – they don’t recognize administrative borders (Matic and Karleusa, 2022).

4. CONCLUSION

There is increasing interest among scientists and practitioners in ecosystem services’ contribution to hydro-meteorological disaster risk reduction. Various measures that increase water retention capacity based on the ecosystem concept are win-win and no-regret measures. Given the increase in disasters generated by hydrometeorological events and uncertainties with respect to future events (floods, storms, heavy rainfall, drought, etc.) frequency and intensity there is a need for an increase in water retention capacity, from small-scale catchments to large river basins. Since they are site-specific due to the natural features of the drainage area, assessment of their application and efficiency has to be hydrology-based and not bureaucracy and administrative boundaries based. on administrative decisions. Any of ESS approach should not be advocated as an innovative or new approach, since some of the measures are applied for centuries. Deliberating on sectorial terminology and ignoring essence very likely will decrease their acceptance by practitioners in all sectors included in disaster risk reduction. They are all hydrological ecosystem services, site-specific and with respect to low-frequency and high-intensity hydro-meteorological hazards have to be considered only as a support of grey infrastructure, not a wizard stick. Ecosystem services concepts and practical assessment should be more integrated in high-schools and universities curricula.

REFERENCES

- Brauman, A.K., Daily C.G., Duarte T., K.T., and Mooney A.H. (2007). The Nature and Value of Ecosystem Services: An Overview Highlighting Hydrologic Services, *The Annual Review of Environment and Resources*, 32:67–98, doi:10.1146/annurev.energy.32.031306.102758
- Centre for Research on the Epidemiology of Disasters and UN office for Disaster Risk Reduction. (2020). Human Cost of Disasters: an Overview of the Last 20 Years. Available from: <https://doi.org/10.18356/79b92774-en> Accessed:2022-03-05.
- Chow V. T., Maidment R. D., Mays W. L. (1986). *Applied Hydrology* (International Edition). McGraw – Hill Series in Water Resources and Environmental Engineering, Book Company, New York, United States of America.
- EM-DAT Guidelines-The international disaster database, Centre for Research on the Epidemiology of Disasters. Available from: <https://public.emdat.be/about/> Accessed:2022-07-15
- Estrella, M. and Saalismaa, N. (2013). Ecosystem-based disaster risk reduction (Eco-DRR): An overview. In *The role of ecosystems in disaster risk reduction*. Renaud.F.G., Sudmeier-Rieux, K., Estrella, M. (eds.), UNU Press, ISBN 978-92-808-1221-3, e-ISBN 978-92-808-7190-6 Tokyo, 513 pages.
- European Commission, Directorate-General for Environment (EC DG ENV), Jaritt, N., Williams, H., Hanus, A., et al. (2016). A guide to support the selection, design and implementation of natural water retention measures in Europe: capturing the multiple benefits of nature-based solutions. Publications Office. Available from: <https://data.europa.eu/doi/10.2779/761211> Accessed:2019-02-09.
- Jevdjevic V. (1956). *Hidrologija I Deo*. special ed, book 4, Hidrotehnicki institut “Ing. Jaroslav Cerni”, Beograd
- Matic, B., Perovic, M., Vulic, D. (2021). Natural water retention measures contribution to integrated transboundary Tisza River Basin Management - Environmental and Flood risk management objectives synergy. In *Proceeding of the International Symposium: Water Resources Management: New Perspectives and Innovative Practices*, Novi Sad, Serbia, 23-24 September 2021, pp 113-117.
- Matic B. B. and Karleusa, B. (2022). Ecosystem-Based Disaster Risk Reduction Framework as a Tool for Improved River Basin Natural Water Retention Capacity and Environmental Hazard Resilience. *Environmental Sciences Proceedings* 21(1): 40. <https://doi.org/10.3390/envirosciproc2022021040>
- Mayfield, C.I., Grover, V.I. and Daley, R.J. (2004). The United Nations Water Virtual Learning Centre: a flexible distance learning Programme for integrated water resources management. *Global Environmental Change – Part A*, 13(4): 331-318.
- Ruangpan, L., Vojinovic, Z., Di Sabatino, S., Leo, L. S., Capobianco, V., Oen, A. M. P., McClain, M. E., and Lopez-Gunn, E. (2020). Nature-based solutions for hydro-meteorological risk reduction: a state-of-the-art review of the research area, *Nat. Hazards Earth Syst. Sci.*, 20, 243–270. doi.org/10.5194/nhess-20-243-2020, 2020. Available at: <https://nhess.copernicus.org/articles/20/243/2020/>
- Srebrenovic D. (1986). *Primjenjena hidrologija*. Tehnicka knjiga, Zagreb

The fifth session of the United Nations Environment Assembly. (2022). The UNEA-5 resolution. Available from: <https://www.naturebasedsolutionsinitiative.org/news/united-nations-environment-assembly-nature-based-solutions-definition#:~:text=The%20UNEA%2D5%20resolution%20formally,effectively%20and%20adaptively%2C%20while%20simultaneously> Accessed:2023-07-06.

U. Nehren, T. Arce-Mojica, A. Cara Barrett, J. Cueto, N. Doswald, S. Janzen, W. Lange, A. Ortiz Vargas, L. Pirazan-Palomar, F.G. Renaud, S. Sandholz, Z. Sebesvari, K. Sudmeier-Rieux, Y. Walz. (2023). Towards a typology of nature-based solutions for disaster risk reduction. *Nature-Based Solutions*, Volume 3, 100057, ISSN 2772-4115, <https://doi.org/10.1016/j.nbsj.2023.100057>(<https://www.sciencedirect.com/science/article/pii/S2772411523000095>)

PERFORMING MOBBING IN THE PUBLIC SECTOR

Leon Vedenik¹

¹ Police Directorate Murska Sobota, Ulica arhitekta Novaka 5, Murska Sobota, Slovenia,
leon.vedenik@policija.si

Received: 29th August 2023

Accepted: 4th September 2023

Professional paper

Abstract: *The most common cause of maltreatment and victimisation of an employee is inadequate management, and most of all not clearly divided accountability and responsibilities. Individuals, who have been exposed to constant mobbing at work for a longer period of time, are less effective than they would otherwise be. Studying and preventing mobbing is of extreme importance since it adversely affects the performance of employees, organisational effectiveness and efficiency. Employees in the public sector face it more and more frequently, and are often left by themselves, which causes a lot of stress and often unexplained sickness absenteeism from work. The article will describe the normative regulation of the area for employees in the public sector in Slovenia and suggests specific solutions.*

Key words: *mobbing, public sector, safety and health at work, Slovenia*

1. INTRODUCTION

Mobbing most often occurs in poorly organised and poorly managed work environments.

Its victims are not only individuals having lower education, weaker character or being underprivileged, but more and more frequently also individuals of above average ability, who are educated, creative and outstanding in all respects. Mobbing is actually systematic bad and unethical conduct in the workplace that includes ridicule, hate speech and psychological terror as such.

In most cases, or almost always, the victim of mobbing is one person, who can be a subordinate worker, or even a superior, but most often it is one co-worker whom work environment isolates, and continuously attacks over a longer period of time. Because of his isolation in the workplace, this individual feels powerless to defend himself or to report to his superior, thus he is being exposed to aggressive and negative behaviour in the workplace for a long time.

The public administration system is an ideal environment for the flourishing of mobbing at all levels due to the closedness of the system, which hinders or even prevents communication, the way of management, which is distinctly hierarchical and can also be authoritative, and because the degree of decision-making by civil servants in the system is very low.

2. NORMATIVE REGULATION OF THE AREA

Article 14 of the Constitution of the Republic of Slovenia stipulates that everyone in Slovenia is guaranteed the same human rights and fundamental freedoms, regardless of nationality, race,

gender, language, religion, political or other belief, financial status, birth, education, social position or any other personal circumstance. All are equal before the law. Article 34 stipulates that everyone has the right to personal dignity and security. Guaranteeing the inviolability of a person's physical and mental integrity, his privacy and personal rights is determined by Article 35.

The umbrella legislation in the field of safety and health at work, i.e. The Act on Safety and Health at Work determines already in the fundamental principles in paragraph 1 of Article 5 that the employer must ensure the safety and health of workers at work. For this purpose, it must implement the measures necessary to ensure the safety and health of workers and other persons present in the work process, including the prevention, elimination and control of hazards at work, informing and training workers, with appropriate organisation and the necessary material resources.

Paragraph 3 of the same article also stipulates that the employer must consider the changing circumstances and implement such preventive measures and choose such work and production methods that will ensure the improvement of the situation and a higher level of safety and health at work, and will be included in all the employer's activities and at all organizational level.

Health promotion at the workplace is defined by Article 6 of the Act, which determines that the employer must plan and implement health promotion at the workplace.

Planning and occupational health and safety are determined by Article 7 of the Act, which stipulates that when planning the work environment, work spaces, work and technological procedures, the use of work and personal protective equipment and the use of hazardous chemical substances, the employer must ensure that all impacts on the safe and healthy work of workers and that the environment, procedures, premises, equipment and substances are suitable and in accordance with the purpose of use.

When planning work, the employer must consider the mental and physical capabilities of the workers and reduce the risks due to workloads that may affect the safety and health of workers at work.

The employer implements the measures referred to in Article 5 of this Act observing the following fundamental principles: avoiding dangers; risk assessment; control of hazards at the source; adapting the work to the individual through the appropriate design of the workplace and work environment, work spaces, work and technological procedures, the choice of work and personal protective equipment and work and production methods, especially by eliminating monotonous work and conditions with an imposed rhythm of work and other health harmful circumstances (humanization of work); adapting to technical progress; replacing dangerous with non-dangerous or less dangerous; developing a comprehensive safety policy that includes technology, work organization, working conditions, interpersonal relations and factors of the work environment; prioritizing collective safety measures over individual ones and giving appropriate instructions and notifications to workers.

Article 24 of the Act determines that the employer must take measures to prevent, eliminate and manage cases of violence, mistreatment, harassment and other forms of psychosocial risk at workplaces that may endanger the health of workers.

Likewise, Article 7 of the Labour Relations Act stipulates that sexual and other harassment at the workplace is prohibited. Sexual harassment is any form of unwanted verbal, non-verbal or physical conduct or behaviour of a sexual nature with the effect or intent of harming a person's dignity, especially when it involves creating an intimidating, hostile, humiliating, humiliating

or offensive environment. Harassment is any unwanted behaviour related to any personal circumstance with the effect or intent of harming a person's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment.

Sexual and other harassment from the previous paragraph is considered discrimination according to the provisions of this Act.

Refusal of the actions referred to in the first paragraph of this article by the affected candidate or worker may not be a reason for discrimination in employment and work.

Mistreatment in the workplace is prohibited. Mistreatment in the workplace is any repeated or systematic, reprehensible or blatantly negative and offensive conduct or behaviour directed against individual workers in the workplace or in relation to work. A worker who is a victim of ill-treatment may not be exposed to adverse consequences as a result of actions aimed at enforcing the ban on ill-treatment at the workplace.

Article 47 of the Act stipulates that the employer is obliged to provide such a working environment in which no employee will be exposed to sexual and other harassment or ill-treatment by the employer, superiors or colleagues. For this purpose, the employer must take appropriate measures to protect workers from sexual and other harassment or from ill-treatment at the workplace.

Article 5 of the Act on the Implementation of the Principle of Equal Treatment stipulates that harassment is unwanted behaviour based on any personal circumstance that creates an intimidating, hostile, humiliating, humiliating or insulting environment for a person and insults their dignity.

Article 15 of the Civil Servants Act stipulates that the employer must protect civil servants from bullying, threats and similar actions that endanger the performance of their work.

Article 15.a of the above-mentioned act determines that any physical, verbal or non-verbal conduct or behaviour of a public servant based on any personal circumstance that creates an intimidating, hostile, humiliating, humiliating or offensive work environment for a person and insults his dignity is prohibited.

The regulation on measures to protect the dignity of employees in state administration bodies, which applies to all employees in the bodies regardless of their position or position and the specifics of their employment contracts, defines in its provisions the concepts of sexual harassment, harassment and ill-treatment.

The regulation sets out measures to prevent sexual and other harassment or ill-treatment. For assistance and information on the measures available in relation to protection against sexual and other harassment or ill-treatment, the head or supervisor designates one or more employees who enjoy the trust of the employees and undergo training in the field of protection against sexual and other harassment, or torture. The tasks of the counsellor from the previous paragraph are to inform the person who has experienced sexual and other harassment or mistreatment about the available procedures, and to help them solve the problem if they ask for it. Information obtained from the abused person may not be used without the consent of the person who has experienced sexual and other harassment or abuse.

If the superior believes that there is a reasonable suspicion that sexual and other harassment or ill-treatment has occurred, or that such conduct or behaviour continues even after informing the suspected person of the inappropriateness of such conduct or behaviour, the superior shall act in the following ways: or take action in accordance with the provisions on disciplinary

responsibility; or impose a measure of regular termination of the employment contract for reasons of fault; or impose a measure of extraordinary termination of the employment contract.

In cases where there is a suspicion that there has been a violation of the prohibition of sexual and other harassment or ill-treatment, which are defined as criminal acts in the Criminal Code, regardless of the provisions of this regulation, the police or the competent state prosecutor's office must be immediately notified of the act.

Harassment in the workplace can also be a criminal act, which is defined in Article 197 of the Criminal Code, namely "Whoever causes humiliation or fear to another employee in the workplace or in connection with work by means of sexual harassment, psychological violence, ill-treatment or unequal treatment shall be punished with imprisonment of up to two years. If the act referred to in the previous paragraph results in a mental, psychosomatic or physical illness or a reduction in the work productivity of the employee, the offender shall be punished with imprisonment of up to three years."

Violation of human dignity through abuse of official position or official rights is dealt with in Article 266 of the Criminal Code, which stipulates that an official who, while performing his duties by abusing his official position or official rights, insults or physically injures anyone or even treats him in a way that affects his human dignity, shall be punished by imprisonment for up to three years.

3. WHAT IS REALLY MOBBING?

The term "mobbing" was coined by the Austrian zoologist, ethologist and ornithologist, "Nobel laureate" Konrad Lorenz, who, while observing animals, came to interesting findings in which ways a group of animals repels or eliminates an intruder or a competitor, and how individual animals participate in this.

A Swedish work psychologist of German origin, Prof. Dr. Heinz Leymann, PhD, who was a lecturer at one of the Swedish faculties, was the first to define the word mobbing as a kind of disturbed communication in the workplace burdened with conflicts, which can be e.g. any kind of ridicule, be it appearance or work ability, also private life, manner of speech or any other hostile act.

He came to the conclusion after he'd been observing at his work the same behaviour of employees in different work environments for several years, and finally gave a professional definition of mobbing. He concluded that mobbing is disturbed communication in the workplace, which is significantly burdened by conflicts among colleagues or among subordinates and superiors, while an attacked person is in a subordinate position, exposed to systematic and long-lasting attacks by one or more persons with the aim of to push him out of the work environment. He defined mobbing in 45 points very precisely, as it must last at least 6 months and must happen at least twice a week.

From the above stated, mobbing can be defined as actual systematic bad and unethical conduct in the workplace, which includes ridicule, hate speech and psychological terror as such.

The most common cause of ill-treatment of an employee is inadequate management, and above all unclearly divided powers and responsibilities. Individuals who are exposed to continuous ill-treatment at work for a long period of time are less effective than they would otherwise be. The study and prevention of ill-treatment is therefore important for it has a negative impact on the employees' capabilities, organisational efficiency and effectiveness.

4. FORMS OF MOBBING

Considering various criteria, especially the position of the perpetrators and victims, and the method of implementation, mobbing can be carried out as horizontal or vertical mobbing.

We speak of horizontal workplace mobbing among peers when one or a group of employees mobs another employee.

Vertical workplace mobbing takes place when a superior mobs a subordinate (an employee), and vice versa, when an employee (a subordinate) mobs a superior.

We can also distinguish four forms of mobbing; these are bullying, bossing, mobbing and staffing.

Bullying is almost vulgar mobbing from the top downward (by the owner or the highest boss), it can be brutal, sometimes connected also with physical violence. In some English-speaking countries, however, they use the word bullying as a general term for mobbing; this definition is especially typical of America.

Bossing is mobbing by a superior, but not in such a brutal form, which of course does not mean that it is less intense. On the contrary, when the boss mobs the victim, there is no chance for the victim to escape from this circle, which means that he is already intended "to be shot"; fighting the boss is extremely difficult.

Mobbing is also called psychological terror between fellow workers who are equal in rank, when a certain group of people gathers to mob an individual, either because of his peculiarities or differences, or because of his above-average ability or extraordinary sense of justice and fairness.

Staffing is a form of mobbing by subordinates against superiors, which most often occurs in public institutions, as well as in companies, when workers want to get rid of a strict boss. When new superiors arrive at the workplace, they are often mobbed by their subordinates, as they do not provide them with the information they need for successful work, ignore their instructions, make fun of them and slander them.

A form of mobbing is also when a worker is assigned work that is harmful to his state of health, or the signing of contracts for women, who by the signing the contract commit not to become pregnant during a certain period and, among other things, sexual harassment at the workplace.

A newer form of mobbing is e-mobbing, which involves illegal hacking into a computer, checking e-mails, copying documents, checking and controlling the websites that the mobbed person visits.

5. VICTIM OF MOBBING

In most cases, or almost always, the victim of mobbing is one person, who can either be a subordinate worker or a superior, but most often it is one colleague whom the work environment isolates and continuously attacks over a long period of time.

Because of his isolation in the workplace, this individual feels powerless to defend himself or to report to his superior, thus he is exposed to aggressive and negative behaviour in the workplace for a long time.

6. HOW TO RECOGNISE MOBBING OR BULLYING

When anyone in the company notices that anything that could be mobbing is happening in their work environment, they must take immediate action. Every employee is responsible for

relations in the company. It is for this reason that every employee has the right and the duty to inform their superiors of observed irregularities or to file a report of mobbing.

The Guidelines for the Protection of Employees from Sexual and Other Harassment and Ill-treatment in the Workplace define maltreatment in the workplace as any repeated or systematic, reprehensible or blatantly negative and offensive treatment or behaviour directed against individual workers in the workplace or in connection with work.

In order to make it easier to recognize ill-treatment in practice, below are examples of some forms of conduct or behaviour that could be defined as ill-treatment:

6.1. Behaviour or conduct that affect the self-expression and the way of communication of the abused person

- a) The superior person, fellow workers limit the possibility of the victim to express himself;
- b) Constantly interrupting his speech;
- c) Yelling at and insulting the abused person;
- d) Constantly criticizing his private life;
- e) Telephone intimidation, oral and written threats;
- f) Preventing contact with looks or gestures and with teasing;
- g) etc.

6.2. Behaviour and conduct that limit and prevent social contacts of the abused person

- a) No one talks to the abused person anymore, as if he is not there, does not exist;
- b) The abused person cannot talk to anyone – it is denied access to others;
- c) Transfer to a workplace that is separate from the others;
- d) It's forbidden for its fellow workers to talk to him;
- e) etc.

6.3. Behaviour and conduct sully the reputation of the victim

- a) Defamation behind her back
- b) Spreading baseless rumours
- c) Ridicule
- d) Treating a person as mentally ill
- e) Ridicule related to mandatory psychiatric evaluation or investigation
- f) Ridicule due to a possible disability or handicap
- g) Imitation of the victim's gestures, way of walking, voice with the intention of mocking
- h) Mocking her political beliefs or religious affiliation, private life and the victim's nationality or ethnicity
- i) She has to do work that affects her self-respect
- j) Her efforts are misjudged and demeaning and her decisions are always questioned
- k) Calling with derogatory names

l) etc.

6.4. Attacks on the quality of the victim's professional and life situation of the victim

- a) Superiors deprive the abused person of important duties
- b) She is assigned tasks that are below her level of professional competence
- c) The victim is constantly given new tasks
- d) The victim's home or workplace is damaged
- e) etc.

6.5. Direct attacks on the victim's health

- a) The victim is forced to perform physically demanding work
- b) Threats of physical violence
- c) Physical abuse
- d) Open sexual harassment
- e) etc.

7. THE COURSE OF MOBBING OR BULLYING

The course of mobbing in different forms takes place in five phases at the workplace. These phases extend from initial unresolved conflicts at the workplace, through the search for excuses for certain actions and demonstrations of power, until the moment when the individual is excluded from the working environment and social contact at the workplace. As we said earlier, there can be several forms of mobbing, which differ depending on who the victim of these psychological attacks is.

8. MOBBING CONSEQUENCES

The consequences of harassment and ill-treatment in the workplace are very terrible for an individual, for work colleagues, for the organisation itself and also for society as a whole.

The most common problems of the "targets" of harassment and ill-treatment at the workplace are manifested in the form of psychosomatic illnesses, which cause absenteeism, turnover, disability procedures, exits from the labour market, which leads to a decrease in the social security of these individuals and their families.

During the time of harassment and ill-treatment at the workplace, due to the psychological consequences, the worker also suffers great damage in the area of the personal social network (loss of colleagues, friends, intimate contacts with loved ones), the wider social network, as well as social reputation; the social exclusion of the individual may also occur. Weak social security and social exclusion are the exact opposite of the goals of the national social welfare programme of the Republic of Slovenia.

For a person who is a victim of mobbing, the consequences are mainly of a psychological nature, falling into depression and even suicide. On the other hand, for this reason, they can be pushed to the edge of society, as they can no longer withstand the pressure at work and they resign without having a guaranteed new job.

Harassment in the workplace often affects socially vulnerable individuals and groups of people who are younger, aged between 15 and 28, women over 40 and men over 50, members of

ethnic and racial groups, single mothers, the disabled and the chronically ill, homosexuals, single persons etc.

9. CONCLUSION

Every organisation strives for success, competitiveness and the achievement of set goals with the lowest possible operating costs. The responsibility for success and good work results lies in the hands of the management. Unfortunately, in today's conditions, employees are overloaded with work and constantly under pressure from their superiors, who even threaten to terminate their employment if they do not achieve the desired results.

The most common cause of employee mobbing is inadequate management, and above all unclearly divided powers and responsibilities. Individuals who are exposed to constant mobbing at work for a long time are less effective than they would otherwise be. Studying and preventing mobbing is therefore important because it has a negative impact on employee performance, organizational performance and efficiency.

Despite the fact that Article 34 of the Constitution of the Republic of Slovenia states that every person has the right to personal dignity and security, the right violated by harassment, in practice the opposite happens.

The legal consequences of harassment are still a relatively unexplored area in Slovenia and Slovenian law. In-depth court practices on these issues are still not enough, since harassment as a criminal act is difficult to prove. The statistics of court proceedings are not in favour of workers, as less than half of court proceedings end in favour of the worker (with a judgment in favour of the worker or a court settlement).

The legislation applicable in the field of civil servants in the public sector in several legal acts already provides for the "protection" of employees against bullying, but in practice it still happens that the field of bullying as a criminal act is very difficult to prove.

Employees are clearly aware that this exists, but they are afraid to report mobbing, mainly because of their overall poor financial as well as economic situation and loss of their jobs.

In public administration, the consequences for the resulting damage are not borne directly by the employer, in this case the state, but by the users themselves, since the material damage caused as a result of mobbing is covered from the state treasury. Therefore, the public sector at the implementation level is not very interested in preventing this phenomenon.

Mobbing in public administration is also facilitated by vaguely defined tasks in internal organizational acts, inconsistency of internal acts with legal and by-law regulations, inconsistency of systematization acts with their actual situation in internal organizational units, and the inappropriateness of assigned tasks in relation to the systematized workplace.

Also, the functions of employees in leading positions in all management functions (lower, middle and top) are too interconnected and are "subject" to existing politics, the influences of which also extend to the judicial branch. Despite the fact that mobbing is happening and it is visible to everyone, if they decide to report it, employees are already doomed to failure in large cases from the very beginning; for this reason, they usually do not even decide to report it, so it is essential that they connect with each other and turn to neutral civil institutional organizations for help and through them try to reach a positive solution for them.

It is precisely because of the fear of failure and the state's step-motherly behaviour towards them that employees do not take advantage of all the legal options they still have, as the procedures are long-term and are also related to the financial situation and excessive

psychological burdens when proving harassment, which is felt in the end as an additional defect on their own health.

REFERENCES

Act on Safety and Health at Work (Official Gazette of the Republic of Slovenia, No. 43/11)
Act on equal opportunities for women and men (Official Gazette of the Republic of Slovenia, no. 59/02 , 61/07 – ZUNEO-A, 33/16 – ZVarD and 59/19)

Bohl T. (2019). Kaj je mobing: opredelitev in pojavne oblike Available from <https://www.e-kadrovik.si/vsebine/varstvo-pri-delu-in-promocija-zdravja/mobing/kaj-je-mobing-opredelitev-in-pojavne-oblike/> Accessed: 18.07.2023.

Constitution of the Republic of Slovenia (Official Gazette of the Republic of Slovenia, no. 33/91-I , 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99, 75/16 – UZ70a and 92/21 – UZ62a)

Criminal Code (Official Gazette of the Republic of Slovenia, No. 50/12 – official consolidated text, 6/16 – corr. , 54/15 , 38/16 , 27/17 , 23/20 , 91/20 , 95/21 , 186/ 21 , 105/22 – ZZNSPP and 16/23)

Individualni delovni spori v zvezi s trpinčenjem na delovnem mestu Available from https://www.sodnapraksa.si/?q=26/2009&_submit=i%C5%A1%C4%8Di&id=49948&rowsPerPage=20 Accessed: 11.07.2023.

Labor Relations Act (Official Gazette of the Republic of Slovenia , no . 21/13 , 78/13 - app . 19 – ZPosS, 81/19 , 203/20 – ZIUPOPĐVE, 119/21 – ZCmIS-A, 202/21 – odl. US, 15/22 and 54/22 – ZUPS-1)

Law on Civil Servants (Official Gazette of the Republic of Slovenia, No. 63/07 - official consolidated text, 65/08 , 69/08 - ZTFI-A, 69/08 - ZZavar-E, 40/12 - ZUJF, 158/20 - ZIntPK -C, 203/20 – ZIUPOPĐVE, 202/21 – odl. US and 3/22 – ZDeb)

Mobing na delovnem mestu Available from <https://www.arag.si/arag-svetuje/mobing-na-delovnem-mestu/> Accessed: 15.07.2023

Regulation on measures to protect the dignity of employees in state administration bodies (Official Gazette of the Republic of Slovenia, no. 36/09 and 21/13 – ZDR-1)

Turk B. J. (2019). Kaj je mobing? Postopek ukrepanja, ce so podani znaki mobinga, kako ga dokazati, predvidene sankcije Available from <https://www.iusinfo.si/medijsko-sredisce/v-srediscu/247018> Accessed: 25.07.2023.

Vedenik, L. (2015). Mobing v javnem sektorju. Management and safety M&S 2015: conference theme: Stress management and safety : program cycle: Modern management concepts and safety : 10th international conference, pp.. 230-231, ISBN 978-953-58000-3-3. Opatija, Croatia, June 12th and 13th, 2015, European Society of Safety Engineers, Zagreb

Weber N. (2021). Vampirji v delovnem okolju - pregled sodne prakse na področju mobinga, Revija Odvetnik, st. 102, 2021. Available from <https://www.iusinfo.si/medijsko-sredisce/v-srediscu/288837> Accessed: 11.07.2023

ANALYSIS OF COMPLIANCE OF VALJEVO DISASTER RISK ASSESSMENT WITH METHODOLOGY

Srecko Vukovic¹, Serif Bajrami^{2a}, Katarina Jankovic^{3b}

¹General Staff of the Serbian Armed Forces, Directorate for Development and Equipping J-5, Technical Test Center, Center for Testing Weapons and Military Equipment, Nikinci, Republic of Serbia, srecko.vukovic99@gmail.com

²University of Defence in Belgrade, Military Academy, Veljka Lukica-Kurjaka 33, Belgrade, Republic of Serbia, bajramiserif@gmail.com

³General Staff of the Serbian Armed Forces, Directorate for Development and Equipping J-5, Technical Test Center, Center for Testing Weapons and Military Equipment, Nikinci, Republic of Serbia, jankovickatarina95@gmail.com

Received: 29th August 2023

Accepted: 10th September 2023

Professional paper

Abstract: *In today's dynamic world, disaster risk assessment stands as a pivotal element in safeguarding and promoting the sustainable development of local self-government units. These units play a crucial role in ensuring the safety of their citizens, environment, and valuable assets, all while confronting increasingly frequent threats, including natural disasters and other hazards. This paper centers its focus on evaluating the alignment of Valjevo's disaster risk assessment with the prescribed methodology and content, including the protection and rescue plan.*

The research aims to deepen our understanding of how the recommended steps of the disaster risk assessment methodology are consistently applied within this specific local self-government unit. Through an examination of how potential risks are identified, assessed, and documented, this paper sheds light on the effectiveness of the disaster risk assessment process and the quality of its outcomes.

Key words: *risk assessment, methodology, disaster, city of Valjevo*

1. INTRODUCTION

In a world facing increasingly frequent natural disasters, technical-technological accidents, and other threats, risk assessment becomes an essential tool for managing these dangers. Local self-government units bear the responsibility to accurately identify, analyze, and respond to potential risks, safeguarding the lives, health, critical infrastructure, and cultural assets of their communities.

^a ORCID: 0000-0002-8504-9430

^b ORCID: 0009-0006-0988-4895

This paper analyzes the compatibility between the risk assessment methodology and the protection and rescue plan within the local self-government unit of Valjevo. By examining the steps in the risk assessment process, the research aims to determine if potential risks are correctly identified, adequately analyzed and assessed, and if response strategies are effectively integrated.

This study can enhance our understanding of the pivotal role of disaster risk assessment in the sustainable development of local communities. The compliance analysis offers valuable insights for improving local-level risk management approaches, bolstering security, and enhancing resilience against unforeseen events that may jeopardize the well-being of citizens, property, and the environment.

2. METHODOLOGY OF CREATION AND CONTENT OF DISASTER RISK ASSESSMENT

The Law on Disaster Risk Reduction and Emergency Management (2018) places greater responsibility on local self-government units, emphasizing their primary role in disaster risk management within their territories (Article 5). The principle of the gradual use of forces and assets dictates that local self-government units should first deploy their own resources in protection and rescue efforts, with involvement from the Republic of Serbia's forces and assets when necessary (Article 6).

Within their territories, local self-government units are responsible for creating risk assessments, disaster risk reduction plans, and protection and rescue plans, which have a three-year validity and require approval from the Ministry of the Interior. These documents must be prepared by authorized companies or by the local self-government unit itself, provided they have at least one permanently employed person with the required license.

The minister responsible for internal affairs prescribes the methodology, preparation method, and content of the disaster risk assessment (Maric, 2006). The entire process includes preliminary actions to determine participants, hazard assessment criteria, on-ground monitoring, and periodic updates post-adoption. The Disaster Risk Assessment methodology encompasses risk assessment, monitoring, determination, analysis, evaluation, and risk treatment procedures.

Risk assessment, as a part of risk management, forms the foundation for developing preventive and operational plans. It is crucial to conduct risk assessments effectively, considering realistic assumptions, available data, and innovative approaches. The risk assessment process follows ISO 31000 and ISO 31010 standards, as depicted in Figure 1.

1) Communication and consultation is a continuous and interactive process that the holder of the Assessment implements in order to provide and share the obtained information and engage in dialogue with stakeholders regarding risk management.

2) Determining the context is defining the external and internal parameters that should be taken into account when creating a scenario in terms of representing the potential, and at the same time, the greatest and most probable risks.

3) Risk assessment is the determination of the nature and degree of risk of potential danger, state of danger and consequences that can potentially endanger the lives and health of people, material goods and the environment. It is a process that includes determination (identification), analysis and evaluation of risks.

4) **Risk monitoring** is a constant check, supervision, critical observation or determination of status, in order to identify the expected or necessary changes of all parameters on which the assessment is based.

5) **Risk identification** is the process of finding, recognizing and describing risks.

6) **Risk analysis** is the process of understanding the nature of risk and determining the level of risk.

7) **Risk assessment** is the process of comparing the results of the risk analysis with the risk criteria, in order to determine whether the risk and/or its magnitude can be tolerated.

8) **Dealing with risk (risk treatment)** is a process that is carried out to modify - reduce risk.

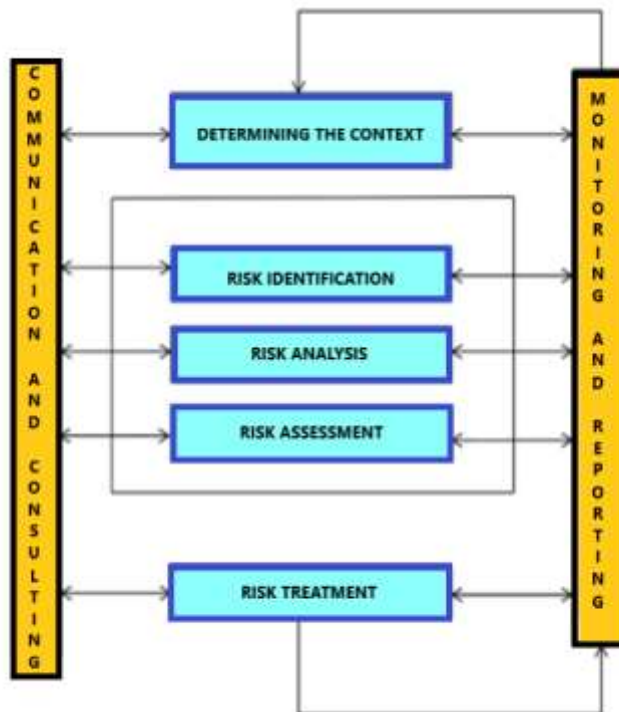


Figure 1. Risk assessment process within risk management

Source: ISO TC 223/SC, 31000: Risk management - Guidance on the principles and implementation of risk management

The aim of disaster risk assessment is to recognize, define, and analyze all aspects related to the current situation, hazards, consequences, risk mitigation, and community responses to natural and other disasters (Smith & Petley. 2009). This includes:

- Description and status of protected values.
- Identification of risks and their root causes.
- Assessment of potential consequences resulting from hazards.
- Determining the suitable organization and implementation of prevention measures.
- Evaluation of requirements and opportunities for providing human and material resources.

Disaster risk assessment in accordance with the Methodology (2019) contains the following parts: Introduction, General part, Special part, Conclusion.

3. DISASTER RISK ASSESSMENT OF THE CITY OF VALJEVO

Reducing the risk of disasters and managing emergency situations is a top priority for all authorities in the City of Valjevo. The area of Valjevo is increasingly threatened by various types of natural hazards, including floods, droughts, earthquakes, landslides, erosion, storms accompanied by hail, heavy snowfalls and drifts, as well as technical and technological accidents, explosions, fires, hazardous substances, and the potential collapse of the "Stubo-Rovni" dam.

Global climate changes in recent years have also contributed to an elevated disaster risk and environmental degradation, leading to adverse effects on human health, the survival of many natural species, and cultural heritage.

The disaster risk assessment for the territory of Valjevo provides an overview of the city's geographical location, hydrographic and meteorological-climatic characteristics, demographic makeup, agricultural production, material and cultural assets, and protected natural resources. Facilities and other critical infrastructure are presented in detail. Furthermore, the assessment identifies and addresses the risks posed by natural disasters and other accidents.

In addition to local and district-level experts, specialists from the Institute for Water Management "Jaroslav Cerni" in Belgrade, the Seismological Institute of Serbia, and the Hydrometeorological Institute of Serbia were involved in the process of identifying disaster risks.

In accordance with the methodology for preparing the Disaster Risk Assessment, scenarios were developed for the most likely adverse events and scenarios with the most severe possible consequences. These scenarios are detailed in Table 1.

Table 1. Identified hazards with possible scenarios (*Valjevo disaster risk assessment, 2022*)

No.	DANGER	SCENARIO	
		The most likely adverse event	An event with the worst possible consequences
1	Earthquake	An earthquake with a magnitude of 5.2 on the Richter scale	An earthquake with a magnitude of 5.6 on the Richter scale
2	Floods	Flooding in the Obnica river basin. The occurrence of large waters with a probability of 1% (Q=240 m ³ /sec) and precipitation of a local character in the basin - 120.00 mm in 24 h	Catastrophic floods in the Kolubara river basin in coincidence with the Gradac river with the generation of other hazards (landslides and landslides)
3	Fires and explosions, open fires	Fire in the attic of a multi-story house in an inaccessible place	A large forest fire in the conifer complex "Maljen-II" in Divcibare
4	Technical and technological accidents	Accident in "HK Krusik" Valjevo	The demolition of the "Stubo Rovni" dam and the appearance of a flood wave

Figures 1 and 2 present summary matrices of identified hazards for the most likely adverse event and the worst-case scenario event.

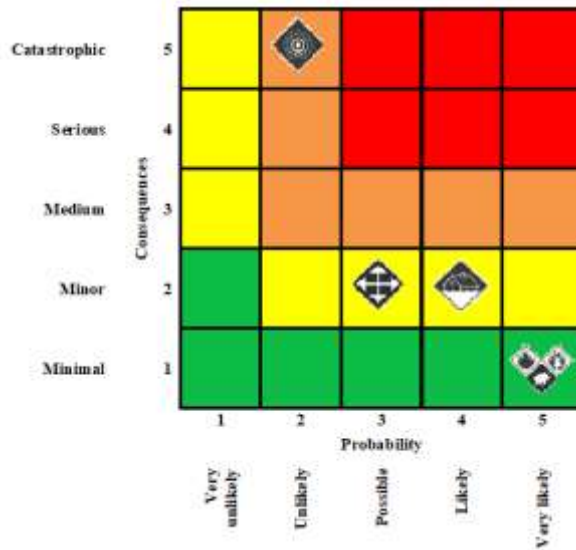


Figure 1. Summary matrix of the most likely adverse event according to the constructed scenarios for the identified hazards
Source: Valjevo disaster risk assessment, 2022

In Figure 1, the risk levels for floods, technical-technological accidents, fires, and explosions are acceptable for the most likely adverse event, while the risk level for earthquakes is unacceptable.

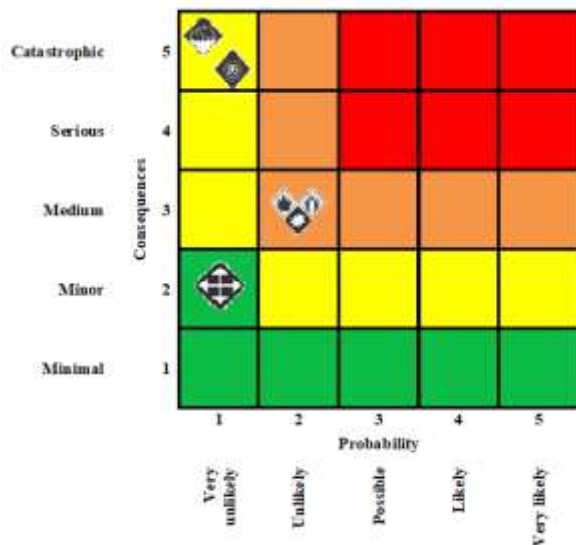


Figure 2. Summary matrix of events with the most severe possible consequences according to the constructed scenarios for the identified hazards
Source: Valjevo disaster risk assessment, 2022

In Figure 2, the risk levels for floods, technical-technological accidents, and earthquakes are acceptable for events with the worst possible consequences, while the risk level for fires, explosions, and open fires is unacceptable.

A risk assessment is a document designed to identify hazards and potential consequences. Its primary goal is to enhance the City's overall capacity for hazard prevention, planned and effective responses to natural disasters and other accidents, damage prevention, and, if unavoidable, minimizing damage to the greatest extent possible.

4. CONFORMITY OF THE DISASTER RISK ASSESSMENT OF THE CITY OF VALJEVO WITH THE METHODOLOGY OF THE CREATION AND CONTENT OF THE DISASTER RISK ASSESSMENT AND THE PROTECTION AND RESCUE PLAN

Upon analyzing the Disaster Risk Assessment of Valjevo, it is evident that all aspects of the assessment align with the prescribed methodology, meeting the national-level requirements and guidelines. The verification of compliance with both the methodology and content of the disaster risk assessment and the protection and rescue plan was carried out through the following points:

1. Application of the steps in the disaster risk assessment: The analysis confirmed that the steps of the disaster risk assessment for the city of Valjevo were correctly and consistently applied in accordance with the prescribed methodology. This included systematic hazard identification, risk analysis and assessment, as well as the thoughtful consideration of response strategies and risk treatment.

2. Content of the Disaster Risk Assessment: The analysis of the Disaster Risk Assessment content confirms that all key components of both the general and special parts are documented and presented in the assessment.

3. Relationship with the Protection and Rescue Plan: The results of the Valjevo disaster risk assessment are clearly incorporated into the protection and rescue plan, with response strategies and the plan itself being based on identified risks and potential consequences.

4. Involvement of interested parties: Relevant stakeholders are actively involved in the disaster risk assessment process in Valjevo, as outlined in the introductory part of the Assessment. Their contributions are documented and integrated into the overall results, demonstrating transparency and comprehensiveness in the approach.

5. Quality of output results: The output results of Valjevo's disaster risk assessments consistently meet the guidelines and requirements of the methodology. Risks, probabilities, consequences, and risk treatments are well-documented and presented.

The disaster risk assessment of Valjevo aligns with national-level methodology and standards, meeting all required guidelines throughout the assessment process. This coordinated approach ensures that Valjevo has a comprehensive and accurate understanding of potential disaster risks, facilitating effective risk management and enhancing overall community safety and sustainability.

5. CONCLUSION

The analysis of Valjevo's disaster risk assessment confirmed that the risk assessment process was systematically and consistently applied, encompassing hazard identification, probability and consequence assessment, and risk treatment. The assessment's content includes all essential components and maintains a clear and transparent link with the Protection and Rescue Plan (Cvetkovic, 2020). Involving relevant stakeholders enhances result integrity and quality.

It's crucial to emphasize that the output results of the risk assessment are precisely documented and well-presented, providing Valjevo with a clear understanding of potential disaster risks.

This forms the foundation for effective risk management, enhancing community safety and sustainability.

The analysis further verified that the risk assessment process is meticulously managed and aligns with guidelines. This alignment is crucial in addressing the growing threats of natural disasters and other hazards. As risk management gains importance, this analysis contributes to a broader understanding of its pivotal role in protecting and promoting sustainable development within local communities.

REFERENCES

Cvetkovic, V. M. (2020). Upravljanje rizicima u vanrednim situacijama. Beograd: Naucno-strucno drustvo za upravljanje rizicima u vanrednim situacijama

Ivanis Z, Babic B, Komazec N. (2016), Security and crisis management-theory and practice: proceedings, Regional association for security and crisis management, Obrenovac

Komazec, N., Randjelovic, A., Pavlovic, S., Mladenovic, M. (2016). Preventive attributes of the risk assessment process in emergency situations, International Risk and Security Consulting and Engineering, Kopaonik, ISBN 978-86-6211-097-8

Komazec, N., Pavlovic, S., Ilic, M. (2014). Risk management as a function of prevention in emergency situations, 16th National Conference "Quality-condition for better business", AKSS, Kopaonik

Maric, P., (2006) Novi institucionalni okviri prevencije vanrednih dogadjaja i njihov znacaj, Bezbednost, br. 4, Beograd

Smith, K.,Petley, D., (2009): Environmental hazardsassessing risk and reducing disaster, Routledge, London and New York.

Assessment of the risk of disasters in the city of Valjevo, Sl. Gazette of the city of Valjevo, February 4, 2022.

Instructions on the methodology and content of the disaster risk assessment and protection and rescue plan, Sl. gazette RS no. 80/2019.

Law on Disaster Risk Reduction and Emergency Management, Official Gazette RS 87/2018

ISO TC 223/SC, 31000: Risk management - Guidance on the principles and implementation of risk management

Nacionalna strategija zastite i spasavanja u vanrednim situacijama "Sl. glasnik RS" br. 86/2011

APPLICATION OF SIMULATIONS IN TARGETING TRAINING

Zeljko Jokic^{1a}, Aleksandar Aleksic², Marko Radovanovic^{3b}

¹ University of Defence in Belgrade, Military Academy, Veljka Lukica-Kurjaka 33,
Belgrade, Republic of Serbia, antras1209@gmail.com

² University of Defence in Belgrade, Military Academy, Veljka Lukica-Kurjaka 33,
Belgrade, Republic of Serbia, aleksic.aleksandar1004@gmail.com

³ University of Defence in Belgrade, Military Academy, Veljka Lukica-Kurjaka 33,
Belgrade, Republic of Serbia, markoradovanovicgdb@yahoo.com

Received: 12th August 2023

Accepted: 16th August 2023

Review paper

Abstract: *Through the definition of shooting with small arms and simulations, the paper presents the process of fire training of soldiers. The importance of applying modern technologies in training through the use of simulation simulators for shooting as a useful teaching tool was emphasized. The VirTra simulation trainer intended for shooting training with rifles and pistols was presented.*

Key words: *shooting, armament, training cours, simulations*

1. INTRODUCTION

The training of individuals and units has always been given great importance. It is believed that in approximately the same conditions, victory in battle belongs to those units that are better trained. For the above reason, training and education were also one of the most important tasks of elders and soldiers in peacetime conditions. Training, as a process of acquiring knowledge, skills and habits, is a vital element in creating conditions for implementing the goals and objectives of the defense system.

The development of technology inevitably influenced the modernization of the army, as well as changes in the way of warfare. For the needs of the war machine, scientific and technological novelties are being developed, which will later be a flywheel in other branches of the economy and society. Of course, all those changes also affected the process of military education.

Fire training, along with tactics, is one of the fundamental subjects in the soldier's training process. Its influence on the trained subject is directly reflected in the final outcome of combat operations. Considering the importance of this subject, it was always approached innovatively. One of the innovations is certainly different types of simulators.

^a ORCID: 0000-0002-3646-1787

^b ORCID: 0000-0002-9866-9639

Simulation trainers have long been integrated into the training plans of foreign armies, where they provide opportunities to create almost realistic training conditions.

In the Serbian Army, simulators have been used in training for many years in different branches and services. Recently, a modern simulation trainer for shooting with an automatic rifle M-70 and pistols CZ 99 and Glock 17 has been available at the Military Academy within the course of Armament with shooting instruction for cadets, listeners for reserve officers and professional military personnel.

The aim of the work is to show the possibilities of using the simulation trainer for shooting with shooting weapons, as well as its contribution to the improvement of teaching in the subject Armament with shooting instruction.

2. SHOOTING WITH ARCHERY WEAPONS

In a broader sense, weapons can be defined as devices for the destruction and incapacitation of the enemy's manpower, its individual and group targets, fortifications and other material assets in wartime conditions, as well as for the defense of the lives and property of citizens in peacetime conditions, as preventive and repressive means of the police and as tools for hunting, fishing and sports. A weapon is also any tool intended for conducting combat operations (Randjelovic & Komazec, 2016).

The criteria for sharing weapons are different. For fire training of soldiers, listeners for reserve officers and cadets of the Military Academy, the most important division is according to purpose, energy source and number of servers. In the following text, firearms will be discussed, with an emphasis on automatic rifles and pistols.

Archery arms are basic, firearms intended for shooting: individual and group live targets (discovered, camouflaged, moving and instantaneous), armored vehicles, bunkers, fortified buildings and fire means. Firearms are part of the equipment of the Serbian Armed Forces, a formation tool of the unit and are personal weapons of members of the Serbian Armed Forces in peace and war. It is prescribed by material formation, and includes semi-automatic and automatic firearms.

Due to their mass use, all units of the Serbian Armed Forces, especially infantry units, carry out training in the field of small arms in accordance with the approved plan and program of training of soldiers and units. Shooting weapons training consists of: theoretical lessons, exercises and shooting.

Within the framework of theoretical classes, the content of knowledge, handling, storage and maintenance of shooting weapons is realized. Through exercises, the necessary knowledge and skills in the field of shooting rules are acquired, and shooting is a test of previously acquired knowledge and the pinnacle of training for a given weapon. They are carried out on simulators and shooting ranges, both closed and open, in accordance with valid instructions and shooting programs for a specific type of firearm.

The process of organizing, preparing and firing a projectile at a target is called shooting (Military Lexicon, 1981). Shooting solves the problem of meeting the projectile and the selected target. That problem involves determining the position and condition of the target relative to the firearm. Based on the specific position and state of the target (in cover, out of cover, in motion, behind the mask...) and the conditions on which the projectile's flight depends (temperature, speed and wind direction), the angle of the barrel and the direction of firing are determined.

Shooting with small arms is a special organizational form of individual training, in which all the knowledge, skills and habits acquired in the training process, during the implementation of lectures and exercises are integrated. Shooting is the most reliable measure of an individual's level of training in solving fire tasks and his combat capability. The importance of shooting is reflected in the efficient (successful) application of small arms fire. Small arms fire is the primary means of neutralizing and destroying enemy manpower on land. The basic principles in the realization of fire are: economy, massiveness, timeliness, surprise, supremacy and elasticity. The success of the application of fire, as a decisive factor in the outcome of combat operations, is evaluated by the material effect (Military Lexicon, 1981).

The goal of shooting with small arms is to train the shooters (soldiers, students, cadets, students of courses for reserve officers and senior officers) for: (Randjelovic & Komazec, 2016)

- proper and safe handling of firearms;
- correct choice and way of shooting different targets;
- economical use of available ammunition.
- execution of fire tasks on command;
- independent, accurate and quick destruction of various targets in combat operations.

Shooting with small arms is carried out under the supervision of the shooting manager - instructor, and in accordance with the rules of shooting with firearms, while respecting certain specificities that distinguish it from shooting with other weapons.

3. SIMULATIONS AND MODELS

The very origin of the word simulation is etymologically related to the Latin word *simulacio* - pretending, obfuscating or otherwise showing the real state than it actually is. In addition to this meaning, simulation is also a method that determines the behavior of systems, models, etc., under changed conditions (Vujaklija, 2004).

According to Shannon (1975), simulation is "the process of designing a model of a real system and conducting experiments with that model in order to understand the behavior of the system or to evaluate different strategies."

Simulation modeling is a complex activity that contains three elements:

1. A real system is an ordered, interdependent set of elements that form a whole and act together to achieve a given goal. The real system is the data source for the model specification.
2. A model is an abstract representation of a system, it gives its structure, components and their interaction. In computer technology, a model represents a set of instructions (program) that serve to generate the behavior of a simulated system. The model has its own objects that are described by attributes and variables.
3. A computer is a device for expressing model instructions, which generate the development of a model in time based on input data. Modeling is the process of establishing a connection between a real system and a model. It refers to model validity which describes how faithfully the model represents the simulation system. Simulation is the process that establishes the connection between the model and the computer. It refers to checking whether the simulation program faithfully transfers the model to the computer and the accuracy with which the computer executes the instructions. Assessing the correctness of the simulator is called verification.

„Simulation is a way of representing the behavior of a real system or the way a real process takes place, by experimenting on a model designed to represent a real system or situation, including those aspects of reality (elements and relationships between them) that are of interest to study. Today, simulation models and simulation experiments are usually developed and used with the help of computers (Jankovic & Nikolic, 2009).

The phrase "modeling and simulation" means a set of activities that construct a model of a real system, after which the dynamics of such a model is simulated on a computer. Each model represents a simplified picture of reality, which does not include all aspects (elements and relationships) of the real system.

In addition to the static structure, each model has its own dynamic aspect, which can be determined analytically, numerically or experimentally. Experimentally determining the behavior of a model is called simulation. If the experiment on the model is done using a computer, then it is a computer simulation, and the model itself, which is then given in the form of a computer program, is called a simulation (Radenkovic et al., 1999; Zeigler, 1976).

The most common areas of application of modeling and simulation in the army are (Radenkovic et al., 1999): Military education, training and practice; Defense planning; Business planning; Procurement of weapons and Research and development.

4. SIMULATION TRAINERS FOR SHOOTING

The purpose of modern simulators is essentially not much different from those of half a century ago. The goal is to create as realistic conditions as possible, that is, adequate simulations for better training. What has made a drastic leap in their production is the technology that has greatly contributed to their importance. Namely, the electronic display of the situation, in addition to other electronic elements, not only physically facilitated the implementation of simulations, but also made additional contributions, such as financial, spatial, temporal, and the most important is the quality of training.

There are different types of simulations that the military uses in their operations. The first type of simulation used in the military is live simulation. This type of simulation consists of systems and people living in a situation where a large group of people participate in a simulated battle. The simulated battle uses real weapons and other equipment used in war. This type of simulation is intended to prepare soldiers for war. It is a real encounter that soldiers experience without necessarily going to the battlefield. The armies of different countries establish specific bases in their countries in order to be able to implement this type of training.

Another application of simulation in the military is the use of virtual simulation. It is one of the most used new technologies in the military. Military personnel use it to train soldiers and pilots to guarantee success on the battlefield. Virtual simulation is used in conjunction with tank simulators used in training soldiers to effectively use tanks on the battlefield.

Virtual simulation has allowed soldiers and tank operators to network and participate in simulated wars even when they are in different locations. Training offered through virtual simulation, i.e. simulation trainers, allows soldiers to participate in exercises, acquire new skills that are crucial in war and raise both individual and collective levels of competence for future combat operations.

4.1. VirTra simulation trainer for shooting with rifles and pistols

Simulation trainers represent a significant step in raising the level of firepower of individuals and units. With the advent of modern information technologies, opportunities for further improvement of simulation trainers have appeared. nRecognizing their application in training,

most of the modern armies of the world began to introduce these teaching aids into training. As demand grew, new simulators appeared on the market. One of them is the American-made simulation trainer called VirTra, which has been available to members of the Military Academy since 2018.

The device allows individuals, shooters, to experience many different situations that they may encounter in real combat through virtual training and shooting. In addition to the basic training of cadets and trainees of the course for reserve officers, the simulator is also intended for higher training, primarily with members of the military police and special units.

VirTra has offered several models to the market, such as: V - ST PRO virtual trainer, V - 100 trainer, V - 180 trainer and V - 300 trainer. For the training of units and individuals in the Serbian Armed Forces, the simulation trainer V - ST PRO is used, which offers a superior training environment.

The system consists of the following components: (VirTra, 2013).

1. The region in which they are located:
 - a) UPS - uninterruptible power supply unit whose task is to enable the operator to safely turn off the computer in the event of a power failure;
 - b) in-line audio amplifier to power overhead speakers;
 - c) computer with Windows 10 operating system and VOS software (version 4.6)
2. Monitor, keyboard and mouse located next to rivers on the table;
3. A screen displaying the selected shooting simulation;
4. High-resolution projector for image broadcasting;
5. High-speed and high-resolution USB camera for detecting laser beams;
6. Tablet for controlling simulations from a distance;
7. WI-FI router for tablet and computer connection;
8. Laser adapters for M-70 rifles;
9. Laser adapters for CZ 99 and Glock 17 pistols;
10. Device for filling frames with compressed CO2 gas.

5. CONCLUSION

Through simulation trainers, a great contribution was made in fire training, which raised its efficiency to a significantly higher level. The ultimate goal of the training is a reflex reaction in a given situation, which demonstrates the psychophysical preparedness of the trained persons as well as their readiness and efficiency in completing tasks. The primary condition for effective response in a given situation is its similarity to training. This is precisely where simulation trainers found their role and became an irreplaceable factor in fire training.

The use of a simulation trainer for shooting with VirTra rifles and pistols has significantly improved the teaching of the subject Armament with the teaching of shooting by members of the Military Academy. Since the simulation trainer has been available to the cadets of the Military Academy, the improvement of their general fire skills is evident.

Further research should be focused on quantitatively determining the improvement in the shooting results of members who use the simulation trainer before combat shooting compared to members who did not have the opportunity to practice shooting on the simulation trainer before combat shooting.

REFERENCES

Jankovic, R., Nikolic, N. (2009). Application of simulations in the study of the physiognomy of modern war, Institute for Strategic Surveillance, Belgrade.

Military Lexicon (1981). VIZ, Belgrade.

Radenkovic, B., Stojanovic, M. & Markovic, A. (1999). Computer simulation, University in Belgrade, Faculty of organizational science, Belgrade.

Randjelovic, A., Komazec, N. (2016). Safe handling of pistols and revolvers, RABEK, Belgrade.

Shanon, R.E. (1975). Systems Simulation – The Art and Science, *Prentice-Hall, Englewood Cliffs*, NJ.

VirTra VTRK GLOK 17/22 CO2 RECOIL KIT MANUAL (2013) - GLOK 17/22 maintenance and installation manual

Vujaklija M. (2004). Lexicon of foreign words and expressions, Prosveta, Belgrade.

Zeigler, B. (1976). Theory of Modelling and Simulation, *John Willy & Sons*, New York.

THE ROLE OF THE SERBIAN ARMED FORCES IN THE SYSTEM OF PROTECTION AND RESCUE IN FIGHTING NATURAL DISASTERS - A CASE STUDY OF THE FLOOD OF 2014 IN THE REPUBLIC OF SERBIA

Serif Bajrami^{1a}, Stefan Pusulic²

¹ University of Defence in Belgrade, Military Academy, Veljka Lukica-Kurjaka 33,
Belgrade, Republic of Serbia, bajramiserif@gmail.com

² University of Defence in Belgrade, Military Academy, Veljka Lukica-Kurjaka 33,
Belgrade, Republic of Serbia, pusulicstefan@yahoo.com

Received: 7th August 2023

Accepted: 14th August 2023

Professional paper

Abstract: *Natural disasters caused by floods, regardless of today's level of scientific development, cannot be completely prevented. They represent the consequences of natural laws on which man has no decisive and direct influence. What can be undertaken, in certain cases, refers to activities aimed at preventing natural disasters or reducing the damage caused. Given the frequency and devastating effect of floods on the territory of the Republic of Serbia, especially in 2005 and 2014, such a question is certainly gaining importance. For the above reasons, the Republic of Serbia was forced to build an effective protection and rescue system in response to the increasingly frequent occurrence of floods and other natural disasters, and one of the most important parts of the above integral system is precisely the units of the Serbian Armed Forces.*

Key words: *flood, protection, rescue and Serbian Armed Forces*

1. INTRODUCTION

In the region of the Republic of Serbia, floods are a periodic phenomenon, different areas are often affected by this natural disaster. The role of the Serbian Armed Forces in the system of disaster risk reduction and emergency management in confronting natural disasters caused by floods is multifaceted, where its basic characteristics such as organization, equipment and training come to the fore. However, units of the Serbian Armed Forces are not the only forces that engage during emergency situations. The Serbian Armed Forces represents only one of the many parts of society whose integration into a unified framework is regulated by normative legal regulations, primarily by the Law on Disaster Risk Reduction and Emergency Management (hereinafter referred to as the Law) (LDRR and EM, 2018).

^a ORCID: 0000-0002-8504-9430

2. THE SYSTEM OF DISASTER RISK REDUCTION AND EMERGENCY MANAGEMENT IN FIGHTING NATURAL DISASTERS

Threats that can lead to catastrophic consequences for the population, material goods and the environment are all kinds of natural disasters to which no country is immune. It is precisely for this reason that the system of disaster risk reduction and emergency management is established in the Republic of Serbia, as part of the National security system of the Republic of Serbia.

Until the adoption of the Law, the role of the individual and the community for responding to the consequences of the disaster, protection and rescue, rights and obligations of both citizens and various organizations in the Republic of Serbia was not clearly defined. Also, with the formation of the sector for emergency situations within the Ministry of Internal Affairs of the Republic of Serbia, an effective risk management system is established, the level of ability to prevent the emergence or mitigation of the consequences of emergency situations is increased, that is, the conditions are created for the integration of all available human and material resources into a unique system intended for an organized and comprehensive response to possible challenges, risks and security threats.

The Law defines such a system, which is based on an integrated form of management and organization of system subjects for the implementation of preventive and operational measures in carrying out the tasks of protecting and rescuing people and goods from the consequences of disasters, including recovery measures from those consequences. The basic elements of the system are subjects and forces defined by the Law as necessary resources needed for the successful implementation of protection and rescue tasks.

Subjects, by their actions, and in accordance with laws and other documents that regulate the organization, development, preparation and use of forces and means of protection and rescue, influence the construction of a unique the system of disaster risk reduction and emergency management in the territory of the Republic of Serbia. The Law on risk reduction recognizes the following subjects: state administration bodies, bodies of autonomous provinces and local self-government units, public services, companies and other legal entities and entrepreneurs, civil society organizations, educational institutions and scientific research organizations, public agencies and others who, in accordance with the law, other general acts, plans, programs and other documents, participate in determining measures and activities of importance for risk reduction and emergency management. (LDRR and EM, 2018: article 13.)

The protection and rescue forces, through their engagement, provide an integrated form of management and organization of the subjects of the system of disaster risk reduction and emergency management for the implementation of preventive and operational measures in the execution of the tasks of protection and rescue of people and property from the consequences of natural disasters and other accidents, including recovery measures from those consequences.

The Law on Disaster Risk Reduction and Emergency Management defines that the protection and rescue forces are responsible for responding in emergency situations and are composed of: emergency headquarters, civil protection units, fire-rescue units, 112 services, the police, the Serbian Armed Forces , the Red Cross of Serbia, the Mountain Rescue Service, the Fire Brigade Association of Serbia, the Association of Radio Amateurs of Serbia, commissioners, that is to say, deputy commissioners of civil protection, citizens, associations of citizens and organizations whose activities are of special interest to the development and functioning of the system. (LDRR and EM, 2018: article 13.)

3. THE ROLE OF THE SERBIAN ARMED FORCES IN THE PROTECTION AND RESCUE SYSTEM

The increasingly frequent occurrence of natural disasters requires, in addition to the usual forces, the active use of units of the Serbian Armed Forces in providing assistance to civil authorities in the joint fight against the devastating consequences caused by strong earthquakes, large floods, droughts and snowfalls. The manner and conditions under which the Serbian Armed Forces are prepared and used in support of civil authorities in the event of natural disasters, technical-technological and other accidents are defined by the Law and doctrinal documents of different hierarchical levels. (Bajrami & Slavkovic, 2016).

In accordance with the provisions of the Law, the Serbian Armed Forces is also recognized as one of the key elements of the aforementioned system. The Law on Disaster Risk Reduction and Emergency Management considers the rational (gradual) use of forces in countering internal security threats by enabling the use of the Serbian Armed Forces in cases where the available forces for protection and rescue are insufficient. (LDRR and EM, 2018: article 6.)

In conditions when other forces and means of the system are not sufficient for the protection and rescue of people, material and other goods from the consequences of disasters, and at the request of the Republic Headquarters for emergency situations, the Ministry of Defense ensures the participation of its organizational units, commands, units and institutions of the Armed Forces to provide assistance in protection and rescue, in accordance with the law, except in a state of war and emergency. (LDRR and EM, 2018: article 26.)

When units of the Serbian Armed Forces participate in protection and rescue, they are commanded by their competent officers, in accordance with the conclusions and recommendations of the headquarters for emergency situations, which manages and coordinates protection and rescue. (LDRR and EM, 2018: article 26.)



Figure 1. a) firefighting by helicopter b) strengthening of embankments

Source: a) <https://www.rtvbn.com/3872410/rs-treba-opremu-za-gasenje-pozara> and b) <https://www.mod.gov.rs/lat/6615/pripadnici-vojske-srbije-angazovani-u-odbrani-od-poplava-6615>

Doctrinal decrees, in addition to war and state of emergency, provide for the possibility of using the Army in secular conditions - emergency situations, in accordance with the law and the decisions of competent state authorities. Making a decision on the use of the Serbian Armed Forces is conditioned by the state of security in the region and the world, the degree of threat to the country, the available defense resources and spatial and weather conditions. (Doctrine of the Serbian Armed Forces, 2010) The basic doctrinal solutions, stated in Doctrine of the Serbian Armed Forces, provide that parts of the Serbian Armed Forces can be put on standby and used (planning, preparation and execution of combat and non-combat operations) in the

event of a declaration of a state of emergency due to natural and other accidents and disasters, based on the decision of the Chief of General Staff or the competent senior officer, and by special authorization of the President of the Republic. (Doctrine of Serbian Armed Forces, 2010) However, for the purposes of providing support to civil authorities, the Serbian Armed Forces does not develop special forces, but uses existing parts of the Army for the purpose of protecting and rescuing people, material and cultural assets from natural disasters, technical-technological accidents, the consequences of terrorism and other major accidents, which, according to the basic purpose, they can successfully perform those tasks. Also, the doctrinal provisions stipulate that the Army, unlike in combat operations where it plays a leading role, in non-combat operations has a supporting role for other forces of the defense system. (Doctrine of the Serbian Armed Forces, 2010) In such circumstances, the success of non-combat operations primarily depends on the achieved level of established cooperation and coordination with the state authorities that lead all the forces in the threatened area and on the level of training and equipment of the units of the Serbian Armed Forces for implementation of non-combat activities (Doctrine of the Serbian Armed Forces, 2010).

4. THE USE OF THE SERBIAN ARMED FORCES IN PROVIDING MOVEMENT TO CIVIL AUTHORITIES DURING THE FLOODS OF 2014

During May 2014, record amounts of rainfall were recorded, more than 200 mm fell in the third week alone, which is the equivalent of three months of rainfall under normal circumstances. The heavy rainfall caused a sudden rise in water levels on the rivers (Sava river, Tamnava river, Kolubara river, Jadar river, Zapadna Morava river, Velika Morava river, Mlava river and Pek river), and the consequences were immeasurable. - landslides, collapsed bridges, collapsed houses, roads and many other damages. All of this made the normal functioning of life in the threatened area significantly more difficult. In such circumstances, the rescue of people, animals, material goods as well as the protection of the environment represented a huge challenge and required the engagement of a large number of people, means and equipment. Among other things, numerous units of the Serbian Armed Forces were engaged, with the aim of providing assistance to civil authorities during the May floods. Forces and resources from the River Flotilla, Special Brigade, 1st, 2nd and 3rd Army Brigade, 2nd and 3rd Training Centar (TC), Rasin Brigade, 5.bMP, TC Lo, Central Logistic Bases and 250th Missile Brigade for AAO made a great contribution to the implementation of search and rescue tasks, the evacuation of the population and the distribution of vital foodstuffs in the flooded area (Bajrami, 2022).

The Serbian Army was engaged in the tasks of protection, rescue and removal of the consequences. The capacities of the Armed Forces are engaged in the area of 12 administrative districts (Moravicki, Kolubarski, City of Belgrade, Podunavski, Macvanski, Rasinski, Zlatiborski, Raski, Branicevski, Pomoravski, Toplicki and Nisavski) in 39 municipalities in 50 locations. Over 2,500 members of the Armed Forces and 185 larger assets (engineering machines, helicopters, boats, amphibious vehicles, motor vehicles) were engaged daily. The forces of the Air Force and Air Force carried out 553 aircraft flights with about 200 hours of sorties (Simovic, 2016).



Figure 2. a) population evacuation b) sanitation of the field

Source: a) <https://www.czkd.org/2014/09/follow-up-obrenovac-je-prisutan> and b) <https://www.blic.rs/vesti/tema-dana/ko-sta-radi-ovo-su-sluzbe-koje-stupaju-u-akciju-posle-poplava/9f81eb4>

Assistance to the civil authorities during the floods in the first phase was provided by the implementation of the following tasks: evacuation of the population, reception and treatment of vulnerable persons, water supply, delivery of food and quartermaster's funds, engineering works on the construction and strengthening of embankments and roads, installation of bridge crossing points, biological decontamination, veterinary supervision, rehabilitation of landslides, water pumping, military-police affairs, medical care and coordination of rescue teams of foreign armed forces (Simovic, 2016).

Table 1. Overview of the engagement of members of the RF during the May floods (Source: Bajrami, 2022.)

Date	Forces to command	Forces to carry out the operation	Forces to logistical support	Total
14.05.	14	92 persons		106
15.05.	26	92 persons		118
16.05.	24	124 persons		148
17.05.	24	169 persons		193
18.05.	26	170 persons	3	199
19.05.	22	114 persons	3	139
20.05.	25	137 persons	3	165
21.05.	25	116 persons	3	144
22.05.	21	121 persons	3	145
23.05.	21	95 persons	3	119
24.05.	5	53		58
TOTAL	233	1283	18	1534

The Serbian Armed Forces hired helicopters, motor vehicles, pumps, boats and water tankers. Members of the army delivered vital foodstuffs, blankets and beds to the vulnerable population. In just one day, they filled more than 2,000 sandbags to strengthen the ramparts. Military forces are engaged in the work of evacuating the captured population, providing medical support and sanitizing the terrain. Members of the ABHO units in cooperation with the veterinary service of the Serbian Armed Forces, the republican veterinary inspection, units of the MUP and the Emergency Staff were engaged in the tasks of cleaning up the biologically

decontaminated area and agricultural goods in the area of the municipality of Ub. Also, in order to prevent the spread of diseases and infections from the contamination of dead animals, fecal waters and contaminated sources of water supply, for sanitation, biological decontamination, disinfection, disinsection and deratization of flooded areas, experts from the ABH service were sent to the field to assist civil authorities.

The River Flotilla of the Serbian Armed Forces made a great contribution in providing assistance to civil authorities during the May floods, especially in the territory of Obrenovac and Sabac. Specifically, for the realization of protection and rescue tasks, the River Flotilla in the period from 14.05. until May 24, 2014, when the intensity of resource strain was at its maximum during the day, on average, it hired about 139 people. The maximum daily stress was on May 18, 2014. year with a total of 199 persons. In total, the River Flotilla had 1,534 daily engagements of its members on tasks from the third mission of the Serbian Armed Forces (table 1) (Bajrami, 2022).

5. CONCLUSION

Previous experiences point to the fact that emergency situations caused by natural disasters such as snowfall, earthquakes and floods were the most common causes of endangering the general safety of our society. A very important place in the fight against natural disasters, especially when it comes to large floods, is occupied by the Serbian Armed Forces with its human, material and organizational capacities. Its contribution is especially expected in the implementation of tasks such as: evacuation of the population, material goods and livestock from areas threatened by floods, primarily by water, and partly by land; aid distribution; isolation of the endangered zone; taking care of the injured and sick; providing medical assistance; rehabilitation of the endangered zone; fire extinguishing; transport; construction of embankments; provision of important hydronavigation facilities on inland waterways; restoration of infrastructure and other activities in a specific emergency situation. As a result of the above, we come to the conclusion that the Serbian Armed Forces, in addition to the fact that it is defined by legal regulations as an entity that provides support, is still recognized as a key element of success in the implementation of the tasks of protecting and rescuing the population and material goods during natural disasters.

REFERENCES

Bajrami, S. (2022). Model of the use of the River Flotilla in the operation of providing assistance to civilian authorities in case of floods, doctoral dissertation, Military Academy, Belgrade.

Bajrami, S. Slavkovic, R. (2016). Doctrinal solutions for the use of the River Flotilla in emergency situations, Војно дело, number. 5, ISSN 0042-8426

Doctrine of the Serbian Armed Forces (2010). Medija centa „Odbrana“, Belgrade

Simovic, M. (2016). Experiences of the Serbian Armed Forces in emergency situations in 2014, Војно дело, number. 6, ISSN 0042-8426

The Law on Disaster Risk Reduction and Emergency Management (2018). SluZbeni glasnik RS, number 87/2018.

SIMULATIONS AND THE QUALITY OF MILITARY EDUCATION

Nenad Komazec^{1a}, Aleksandar Milic^{2b}, Aleksandar Petrovic³

¹ University of Defense in Belgrade, Military Academy, Veljka Lukica Kurjaka 33,
Belgrade, Republic of Serbia, nenadkomazec@yahoo.com

² University of Defence in Belgrade, Military Academy, Veljka Lukica Kurjaka 33,
Belgrade, Republic of Serbia, milickm5@gmail.com

³ University of Defence in Belgrade, Military Academy, Veljka Lukica-Kurjaka 33,
Belgrade, Republic of Serbia, ale_petrovic@live.com

Received: 6th September 2023

Accepted: 12th September 2023

Review paper

Abstract: Education is a key activity in the development of society. According to the needs of the development of modern society, education evolves and requires adaptation, improvement and innovation. Key features of modern education are cost and quality. It is imperative to reduce costs and at the same time increase quality. A modern tool, based on information and communication technologies, which enables the increase in the quality of the educational process and the reduction of costs, are simulations. The essence of simulations, in addition to reducing costs, is the acquisition of knowledge and skills, using improvised platforms, with as realistic a picture of reality as possible. In addition to economic elements, simulations require active engagement of all participants in the teaching process, activation of ideas and problem solving. Such an approach leads to constant improvement of the simulations themselves, work methods, knowledge and the entire education process. The paper discusses the application of simulations in the educational process, from the aspect of improving and acquiring new knowledge and determining existing ones. Although still an under-researched area, there is a solid number of works that point to the importance of simulations in the educational process. By analyzing the existing literature, the authors conclude about the degree of development of simulations and their applicability in the educational process, point to the educational capacity of simulations and the need for their development in all areas of social life. Considering the wide range of different views of the authors on simulations, the authors have carefully analyzed the literature, with the aim of proving the applicability and usability of simulations, while respecting the evidence of the existence of shortcomings. In the conclusion, an overview is given of the need for further study of simulations in the function of innovation and improvement of the education process.

Key words: simulations, education, knowledge, skills, development

^a ORCID: 0000-0001-9227-118X

^b ORCID: 0000-0002-2642-0340

1. INTRODUCTION

Education is a process of planned and organized influence on people, which includes the adoption of a certain system of scientific knowledge and the formation of a scientific view of the world, the development of interest and desire for self-education and the development of mental abilities (Teodosic, 1965). That is, education is the process of acquiring knowledge, skills and habits, developing on that basis understandings, beliefs, attitudes and practical actions, as well as certain personality traits (Kolar, 1967). In addition, education and training are one of the key activities of human resources management in the organization (PrZulj, 2000). Education makes it possible to change and improve the life of an individual and the social community. Educational needs occupy a significant place in the system of human and social needs, while education and knowledge are the key resources of the future that will determine the nature of human relationships. Educational needs cannot be separated from the development process (Ilic, Janjic, 2019), and the development process from the learning process. In this sense, the whole life is learning, so education has no limitations in duration (Simeunovic, 2000). Information and communication technologies bring new opportunities to the world of knowledge acquisition. Namely, computer technology, robotization, automation, virtualization, data transfer in real time, etc. they made it possible to simplify and present the problems of education in a different way. Simplification implies simplification to an acceptable extent, so that the basic characteristics of the simulated system are not lost in the model.

2. ORIGIN AND DEVELOPMENT OF SIMULATIONS AND SIMULATION MODELS

The development of simulations is directly related to the creation of "simulators", devices, programs, i.e. built systems that perform simulations. Simulators are intended for training people in managing real technical systems (Penzer et al., 2001). The appearance of the first "real" simulators, related to the training of riders, dates back to the Middle Ages and the training of knights in combat. War games, challenging and outwitting opponents, on the battlefield are centuries old. Their effectiveness was particularly evident in the training of the Roman legions. That modeling helped make the Roman army the largest the world had seen for almost 2,000 years (500 BC - 1500 AD). War games, as a type of simulation model, were developed in Europe by the Prussians at the end of the 18th and the beginning of the 19th century. Already in 1824, war games were incorporated into the training of the Prussian army. At the end of the nineteenth century, Major V.R. Livermore introduced modern war games to the US military. In 1883, he translated the German (Prussian) rules on war games, which they made based on the experiences of the American Civil War and the Prussian wars they fought in 1866 and 1870-1871. years.

Simulation models represent a simplified and abstract image of a real system. The model is a representation of the system with all the characteristics perceived by the person simulating the system (ZiZovic & Pamucar, 2019). The simplified image of the model depends on the level of abstraction of the observed system. The basic idea of the simulation model is to imitate a real system. An important element of the simulation is the environment. The environment when simulating a real system must match the goals of the simulation and reality as much as possible.

The simulation allows the participants of the simulation, an interactive relationship with the system based on the steps that need to be taken in order to solve the given problem (Lounce, 2004). The simulation environment plays a significant role in the learning process of the simulation participants, because the information obtained is used to improve the characteristics of the simulation, thereby improving knowledge and the learning process.

3. CONCEPT AND CHARACTERISTICS OF SIMULATIONS

Simulation is a way of displaying the behavior of a real system or the way a real process unfolds through experimentation on a model that is made to represent a real system or situation, including those aspects of reality (elements and connections between them) that are of interest for study (Jurisic, 2021). Simulation is, therefore, a state in which we represent something with the help of something else, that is, in which we pretend that something is as if it were something else (Afric, 1999). That is, simulation is "the operation of the model as a function of time (i.e. starting the model to work and monitoring the behavior of the model by recording the values of the selected quantities) (Jankovic & Nikolic, 2019)." There are several basic types of simulations: constructive simulation, virtual simulation and live "vivo" simulation.

Constructive simulation represents scientific-research simulation as a method of operational research. In this type of simulation, the executors have simulated the activities and assets and the environment, so that there is no impact on the output results of the simulation when it is started. This type of simulation is suitable for analyzing certain concepts, predicting certain results, practicing working under stress, making certain measurements, generating statistical indicators and performing analyses (Pamucar et al., 2016).

Virtual simulation implies the use of virtual means to perform certain activities, and it is easiest to demonstrate this through various simulators, e.g. fire fighting, driving, etc. In these simulations, the human is in the focus and in these types of simulations, motor skills (skills such as piloting a plane, steering a ship), decision-making abilities in certain conditions, as well as the ability to communicate and coordinate with the environment are practiced.

Live simulation implies the use of means and people that are real, but the effects are simulated (simulating actions in the case of a chemical accident, a traffic accident, etc.). These are essentially training activities of various services, such as the army, police, firefighters, on dedicated ranges where real equipment is used, in an approximate environment in which they operate and the activities are almost identical to those in reality.

4. ADVANTAGES AND DISADVANTAGES OF APPLYING SIMULATIONS

The question arises of the applicability of simulations to different areas of social life. Most researchers and authors in this field agree that there is no limit. If it is profitable and contributes to the improvement of the characteristics of the organization, simulations can be applied (Milosevic et al., 2021). A particularly significant application of simulations is in the case of phenomena (events, situations) whose way of creation, development and effects cannot be shown realistically (eg, natural disasters, experiments that can endanger life, etc.). Therefore, the application of simulations has its positive and negative characteristics.

The positive aspects of simulation are: reduction of organizational costs, reduction of safety risks for training participants, the possibility of a greater number of repetitions of certain actions (parts of the studied area), the possibility of adjustment and adaptation of conditions as close as possible to real ones.

Cost reduction refers to: impact on people (life and health, level of acquired knowledge), impact on material resources, impact on the environment, impact on the organization and impact on social conditions (Pamucar & BoZanic, 2019). Bearing in mind the above-mentioned impacts, simulations can significantly contribute to reducing costs through: increasing the level of safety of people in training, increasing the level of acquired knowledge, motivating people, spending less material resources, improving the organization through noticing mistakes and learning through simulations, developing awareness in the social community or organization.

Reducing security risks refers to the application of simulations in high-risk professions (construction, mining, military, police, traffic, etc.). Simulations aim to generate or improve knowledge, in conditions that do not affect the life and health of people and the environment.

Simulations as a didactic tool have certain disadvantages. According to Heineke and Meile (Heineke, Meile, 2000) some of them are:

- the "game" scenario is a model of reality, which means that it was created as a simplified,
- decisions in the simulation are made without responsibility, the outcomes of the simulation do not affect the condition of the participants or other people in the real world (e.g. financially),
- the game describes only some selected aspects and concepts from reality, so that education is limited only to parts of knowledge or skills that are taken into account in the game scenario,
- participants can understand the simulation as a game and entertainment rather than education,
- due to the lack of responsibility for decisions and the perception of simulation as entertainment, the behavior of game participants may differ significantly from their behavior in real life.

Bearing in mind the mentioned shortcomings, the teacher has a significant role in the educational process. Just as learning itself and students have faced great changes, it is inevitable that teachers, college professors and lecturers will face them during their approach to work (Holmes, Gardner, 2006). Lecturers are no longer required to use only a textbook, but also a regular evaluation of their resources: searching, evaluating, planning, implementing and managing them in order to provide the best learning outcomes. Learning based on simulations allows both parties, the lecturer and the student, to enrich their teaching and learning experiences through a virtual environment that supports not only the transfer of knowledge, but also research and its application (Komazec et al., 2014).

5. IMPLEMENTATION OF SIMULATIONS IN THE EDUCATION PROCESS

The essence of simulations is learning. Regardless of whether it is a dedicated simulation for learning a specific subject, or simulating the environment for any reason, at the end of the process, information and results are obtained as a result of learning, which serve to make decisions and increase knowledge. The rapid development of information technologies led to the development of software simulations and their use in teaching in order to improve the traditional, ex-cathedra, way of education and adapt it to modern requirements and trends (Plecic, 2017).

Various studies have shown that simulations improve learning outcomes by connecting abstract concepts to concrete experience and enabling participants to gain a better understanding using active learning and problem solving (Hunzeker, Harkness, 2014). Since simulations represent real-life situations, they have choices and limitations that reflect real problems (Prensky, 2001), and in many situations it has been shown that carefully designed and tested simulations can be extremely powerful educational tools (Finkelstein et al., 2005). Simulations represent one of the most effective ways of learning higher order skills: analysis, synthesis and creation of new knowledge (Leger et al., 2011).

Based on the existing literature on business simulations and games, they are used to study many disciplines/sciences (Andreu, Garcia, 2014): engineering, military sciences, administration and political sciences, economics, business, marketing, international relations,

management , foreign languages, medicine, chemistry, mathematics, physics, social and emotional learning, and even in teaching ethics (Buck, 2013). Their contribution to experiential learning and creating empathy for real life situations is a vital component of entrepreneurial education (Akerman, 2011).

6. SIMULATIONS IN THE PROCESS OF HIGHER EDUCATION

Simulations have been applied in the process of higher education for the last decades. Significant application is achieved through the development of computers and information technology (Kundra & Sureka, 2016). The peak is achieved with the introduction of the Internet and information and communication technologies (BoZanic et al., 2016). The basic characteristics of simulations in the higher education process are (Kincaid & Westerlund, 2009): applicability for all categories of persons who learn to emphasize knowledge; help to analyze and perceive the complexity of phenomena and relationships in the environment; enable the study of mathematics, science and technical skills in an applied, integrated way; provide realistic training and acquisition of skills in various fields, especially in science and industry; reduced cost price and security risks for the participants are reduced, ie excluded.

Simulations, in addition to the basic postulates in education, also generate additional values (Zhang & Liu, 2018). The applicability of the findings that arise in research processes is especially emphasized (Gilbet & Troitsch, 2005).

Abstract learning quantitative skills is less effective than learning them in the natural context of decision-making. It is known that simulations can influence the improvement of students' quantitative and financial skills (Vos & Brennan, 2012). They find use value not only in university teaching, but also for training human resources in companies. Simulations increase motivation to learn and encourage explicit and implicit knowledge through visualization of the problem at hand. The activities of the participants are interpreted into action in the very structure of the simulation, which, like an operating system, leads to the fact that complex cause-and-effect relationships between goals, resources, results and consequences of actions, i.e. decision-making, can be seen more clearly. Therefore, the simulation method requires competence in introduction and coordination in future education that encourages independent and creative learning. But what is common to all who use simulations or similar learning methods is the desire to face the challenges of the future in the best possible way (Schwagele et al., 2014).

7. SIMULATIONS IN PRACTICAL TEACHING

A special type of teaching is practical teaching, i.e. acquiring skills. Depending on the activity in which the practical teaching is carried out, this type of teaching can be simple (eg cooking) to very complex (eg military training, pilot training, car driver training, etc.). Simplicity or complexity implies different criteria: number of classes, presence of danger, number of participants, number of repetitions, complexity of the environment, etc. The very fact that it is a practical lesson indicates that in addition to people, the means on which people are trained and qualified (plane, ship, etc.) and facilities (spaces) where the means are used (airport, port, part of the city, etc.)). With simulations, a large part of the influence of assets and objects (spaces) is excluded or reduced, which implies a smaller impact on people and assets, objects (spaces).

The introduction of simulations oriented towards the aspect of acquiring skills is not something new. Simulation oriented towards the conceptualization of the competence model (Karl, 2012) (capabilities) is a model developed for the training of civil engineering students and professionals, but with the intention of inspiring other fields as a transferable and universally applicable method. Competency methods are: competency testing (at the end of the

simulation), self-assessment (online self-assessment at any time) and third-party assessment (by the instructor during the simulation) (Geuting, 2000). In this way, reliable measurements of the effectiveness of the acquisition of skills/competencies can be obtained, which would not be possible to do on the basis of subjective evaluation or self-assessment. In addition, this multi-faceted measurement method reduces the risk of misjudgment for the entire group.

8. SIMULATIONS FOR RESEARCH PURPOSES

Research is a special form of learning, which confirms existing knowledge and generates new knowledge (new knowledge can also be a refutation of existing knowledge). A large number of persons or individuals participate in the research process, depending on the complexity of the research subject. It is very difficult to create a real system in a simulated environment. Learning through simulation in research processes gives precisely the possibility of improving knowledge through attempts, i.e. adjusting the simulation based on the conclusions from the previous iteration. Namely, research is the foundation of scientific knowledge. The task of science is to expand and consolidate acquired knowledge about the world (environment), to provide ever more complete explanations of phenomena and thus help in solving the cognitive and practical problems that people face (Popadic et al., 2018). There are different ways of arriving at the truth, but scientific truth is arrived at exclusively through the application of scientific methods. The scientific method enables science to persevere in its intention to find out the truth in a manner applicable to every occasion, place and time, adapted to that place, occasion and time. The scientific method, in such a way, enables the survival of science. The seriousness of scientific research, therefore, is obvious as well as the need to make the conditions for research as realistic as possible. There are a large number of cases when it is not possible to conduct real research, in which case simulations are used. Although, by their meaning, they refer to the imitation of a real system, simulations intended for scientific research must apply the scientific method. Considering this fact, building a simulation of a real system in the initial period can have many disadvantages, scientists have an obligation to carefully build simulations based on scientific methods.

Simulation is a powerful and important tool for researchers, because it provides the possibility to evaluate projects, plans and/or policies without experimenting on a real system, which can be extremely expensive, time-consuming or simply impractical. It provides answers to possible questions about the system, and thus the costs of field tests, prototypes, etc. are reduced (Budimir, 2013). All of these possibilities to explore possible scenarios and test hypotheses make simulations an important tool in science education.

9. CONCLUSION

The future of education lies in the application of simulations. From the analysis of works in this field, it can be concluded that the authors agree that simulations have a large number of advantages and very few disadvantages. The fact is that they are an interactive educational tool whose motivating environment creates a great similarity with the real environment. The application of modern information technologies, in addition to the impact on business, also reflected on education, which took on new aspects, methodology and ways of generating knowledge. In education, it has long been accepted that participants should be encouraged to actively engage in the teaching process, and thus simulations are a technique of active learning. The use of simulations implies a simulated environment in which decisions are made at the level of specific periods. Simulations influence participants to engage more than classical methods such as reading or following lectures. They provide a more realistic environment and create connections between participants in which they experiment with different roles.

The field of application of simulations in education has a tradition, but will gain importance in the future. Future research should focus on the interaction of humans, machine learning and the environment. The symbiosis of these three factors gives quality in bringing the simulations closer to the real environment. It is of particular importance for simulating systems with an increased risk for the safety of simulation participants.

REFERENCES

Andreu-Andrés A., García-Casas M. (2014). Gaming in Higher Education: Students' Assessment on Game-Based Learning, 45th Conference of the International Simulation and Gaming Association, Dornbirn.

Božanić D., Pamučar D., Komazec, N. (2016). „Application of the fuzzy AHP method in Risk Assessment in the selection of navigation directions of the Serbian Army in flooded areas“, Security and Crisis Management - Theory and Practice, Obrenovac, 29-30. September 2016, Proceedings.

Budimir M., (2013). Uloga novih tehnologija u procesu odlucivanja, Ekonomski vjesnik, God. XXVI, BR.

Buck, W. (2013). Business Ethics Simulations: The Role of Reflection, Intentionality and Assessment, Society for Business Ethics 2013 Annual Conference, Miami, Dostupno na: https://www.academia.edu/3567938/Business_Ethics_Simulations_The_Role_of_Reflection_Intentionality_and_Assessment

Finkelstein N. D., Adams W. K., Keller C. J., Kohl P. B., Perkisn K. K., Podolefsky N., Reid S. and LeMaster R. (2005). When learning about the real world is better done virtually: a study of substituting computer simulations for laboratory equipment, Physical Review, Special Topics: Physics Education Research

Gilbert N. & Troitsch G.K. (2005). Simulation for the Social Scientist – Second Edition, Open University Press

Heineke, J., and L. Meile. (2000). Classroom service games, presentation at the Decision Sciences Institute Annual Meeting, Orlando, FL

Holmes B., Gardner J. (2006). E-learning concepts and practice, Sage publications, London

Hunzeker M. and Harkness K. (2014). The Strategy Project: Teaching Strategic Thinking through Crisis Simulation, PS: Political Science & Politics

Илић, Б, Јањић, Н. (2019). Унапређење квалитета наставе применом рачунарског моделовања и симулације процеса, XXV скуп трендови развоја, квалитет високог образовања, Копаноник, 11.-14.02.2019., папер Но. 1.3-13

Јанковић, Р. и Николић, Н. (2009). Примена симулација у проучавању физиономије савременог рата, Институт за стратегијска истраживања, Београд.

Jurisić, D. (2021). CAH u sistemu zaštite i spasavanja, Bezbjednosni istraživački centar, Banjaluka

Karl, C. K. (2012). Additional Benefit through Competency-Oriented Business Simulations. Developments in Business Simulation & Experiential Exercises, 39.

Kincaid J. P. & Westerlund K. K. (2009). Simulation in education and training, Winter Simulation Conference Колар, З. и др. (1967). Основи војне андрагогије, ВИЗ, Београд.

- Komazec N., BoZanic D., Mihajlovic Lj. (2014). „Aspects of Decision-making in Emergency Situations“, ICT Forum 2014, Nis, 14-16. October 2014, Proceedings, 2014.
- Kundra, D., Sureka, A. (2016). An experience report on teaching compiler design concepts using case-based and project-based learning approaches. u: IEEE Eighth International Conference on Technology for Education (T4E), IEEE
- Lunce M. L. (2004). Computer Simulations in Distance Education, International Journal of Instructional Technology & Distance Learning, Vol. 1. No. 10.
- Milosevic, T., Pamucar, D., Chatterjee, P. (2021). Model for selecting a route for the transport of hazardous materials using a fuzzy logic system. Military Technical Courier, 69(2)
- Pamucar, D., BoZanic D. (2019). Selection of a location for the development of multimodal logistics center: Application of single-valued neutrosophic MABAC model, Operational Research in Engineering Sciences: Theory and Applications, Vol. 2 No. 2 doi.org/10.31181/oresta1902039
- Pamucar, D., BoZanic, D., Komazec, N. (2016). Risk Assessment of Natural Disasters using Fuzzy Logic System Type-2, Management - Journal for Theory and Practice Management, 21(80), 23-32. DOI: 10.7595/management.fon.2016.0016, ISSN 0354-8635
- Penzer D., Srblijinovic, A.i Skunac O. (2001). Kompjuterske ratne igre: borbeni modeli i simulacije razlicitih rezolucija, Polemos 4, ISSN: 1331-5595.
- Plecic, K. (2017). Razvoj novog modela primene poslovnih simulacija u visokoskolskom obrazovanju, doktorska disertacija, Univerzitet Singidunum.
- Premsky M. (2001). Digital Natives, digital immigrants
- Premsky, M. (2001). Digital game-based learning, McGraw Hill, New York
- PrZulj, Z. (2006). Osnove menadzmenta ljudskih resursa, Fakultet za poslovni inZinjering i menadzment, Banja Luka
- Simeunovic V. (2000). Obrazovanje u ratu, Srpsko Sarajevo: Zavod za udZbenike i nastavna sredstva Republike Srpske.
- Schwägele S., Zürn B., Trautwein F. (2014). Planspiele - Erleben, was kommt Entwicklung von Zukunftsszenarien und Strategien, Norderstedt: Books on Demand GmbH,
- Teodosic, R. i dr. (1965). Pedagogika, Zavod za izdavanje udZbenika, Sarajevo
- Vos L. & Brennan R. (2012). How much do simulation games improve marketing students' numeracy and financial skills?, Final report on an Academy of Marketing Teaching & Learning Development Grant
- Zhang, W., Liu, J. (2018). Application of simulation software in analog electronic technology teaching. u: DEStech Transactions on Social Science, Education and Human Science, (ICESSH 2018)
- ZiZovic, M., & Pamucar, D. (2019). New model for determining criteria weights: Level Based Weight Assessment (LBWA) model. Decision Making: Applications in Management and Engineering, 2(2)

FOREST FIRES AND CLIMATE CHANGES IN THE REPUBLIC OF SERBIA

Jelena Lazarevic¹, Nikola Vukojevic², Jovica Milicevic³

¹ University of Defence in Belgrade, Military Academy, Veljka Lukica-Kurjaka 33,
Belgrade, Republic of Serbia, jcrvenkov@gmail.com

² University of Defence in Belgrade, Military Academy, Veljka Lukica-Kurjaka 33,
Belgrade, Republic of Serbia, nikola_vukojevic@ymail.com

³ University of Defence in Belgrade, Military Academy, Veljka Lukica-Kurjaka 33,
Belgrade, Republic of Serbia, jovicamilicevic74@gmail.com

Received: 26th August 2023

Accepted: 10th September 2023

Professional paper

Abstract: *Nowadays, natural disasters represent an increasingly serious problem for humanity. The consequences, after their occurrence, are reflected in human losses, material and non-material damage. Forest fires, as natural disasters, represent the most extreme form of forest devastation, and lead to its complete destruction. In all regions of the world, changes in the regime of air temperature and precipitation were observed, as well as significant variability and changes in other climatic elements. The occurrence of forest fires depends on a number of factors, and one of them is the weather, the state of humidity and the amount of combustible plant material, as well as human activities. The connection between climate change and the increasing number of forest fires is obvious.*

Forest ecosystems are exposed to the adverse effects of climate change, they are a significant carbon reservoir and an important potential for mitigating global warming, which is why they require a special management method that includes protection, improvement of the existing condition and establishment of new forests.

Protecting forests from forest fires, especially in extreme climatic conditions suitable for the occurrence of fires, is one of the most important goals of the entire society, considering the importance and functions of the forest.

Key words: *natural disasters, forest fire, climate change, risk management*

1. INTRODUCTION

Forests are a resource of incalculable importance for life, they play a key role in oxygen production and air purification, they mitigate the effects of climate change. In addition to ecological, forests also have economic and social importance. However, despite the fact that forests represent the lungs of our planet, man contributes to the degradation and disappearance of this resource with his daily activities.

Serbia is considered a medium-wooded country. According to the data of the Republic Institute of Statistics from 2020, as many as 2,261,386 ha are under forest, i.e. 29% of the total territory of the Republic of Serbia (without data for AP KiM).

In the first part of the work, the basic concepts of forest fires and a short research on forest fires that occurred in the Republic of Serbia in the period from 2012 to 2021 were analyzed. The research was conducted by analyzing the data of the Republic Institute of Statistics, ie Forestry Statistics. In the second part of the paper, an overview of the impact of climate change in the world and its basic characteristics on the territory of the Republic of Serbia is given. The third part connects the previous two units and presents an analysis of the obtained data and indicates the negative impact of climate change on forest fires. At the end, preventive measures to protect against forest fires were given.

2. FOREST FIRES

According to the Law on Fire Protection, a fire is defined as a process of uncontrolled combustion that endangers the life and health of people, material goods and the environment. A forest fire is an uncontrolled, spontaneous movement of fire across the forest surface and represents one of the most destructive natural forces (Aleksic & Jancic, 2011).

If we look at the place where the forest fire developed, we distinguish three types of fires, underground, ground and crown fires (crown/high). Forest underground fires are fires that take place without flames, which most often occur in dry underground deposits of peat. Progress is slow, they are difficult to detect and can quickly turn into an open surface fire. Ground fires are the most common type of forest fires, especially in deciduous forests. In the case of ground fires, the fire most often affects dry grass, bushes and dry trees. High fires are usually accompanied by strong winds, they spread quickly, because the fire quickly moves from one tree canopy to another and is difficult to extinguish. Most often, a ground fire is an integral part of a high fire, and burning tree tops without a ground fire is rare. High fires most often occur in the summer, when drought and strong winds can completely destroy affected trees (Aleksic & Jancic, 2011).

Damage from forest fires occurs in the entire ecosystem (plants, animals, soil). After a fire, we very often note the escalation of other destructive factors, such as the proliferation of insects and plant diseases, which further destabilize burned and unburned areas, thereby increasing the area without forest, and the reduction of areas under forest increases the risk of torrential flows in mountainous areas and floods in the lowlands, microclimatic changes, etc.

The consequences of forest fires are economic and ecological. Economic damages include fire extinguishing, reclamation and restoration of the destroyed forest. Environmental damage manifests itself over many years, and the damage that occurs after a fire is incalculable. In the world, it is a practice to calculate them as five or ten times the value of direct damages (Aleksic et al., 2011).

2.1. Forest fires in the Republic of Serbia

The analysis of statistical data on forest fires shows that the frequency of fires, as well as the total burnt area, increases from year to year. The increase in fire hazards and damage can be linked to climate change. Considering the climate scenarios that predict an increase in average temperatures of 4-6°C by the end of this century, a decrease in the total amount of precipitation and its uneven distribution during the year with long periods of drought during the summer, an additional increase in the frequency and burned areas in the territory of Serbia can be expected (Assessment of the risk of disasters in the Republic of Serbia, 2017).

Forest fires occur throughout the year, but three critical periods can be distinguished in our country: March - April, July - August and October - November. It is believed that about 95% of fires are caused by humans due to their own activities (negligence, inattention, and even deliberate burning), so that the daily rhythm of forest fires coincides with the daily activity of humans.

Table 1: The total number of forest fires by origin in the state forests of the Republic of Serbia in the period from 2012 to 2021 (*Source: Authors*)

Year	Place of origin		In total
	Down to earth	Tall	
2012	211	71	282
2013	37	6	43
2014	9	3	12
2015	38	9	47
2016	29	1	30
2017	59	10	69
2018	11	174	185
2019	32	9	41
2020	23	3	26
2021	29	5	34
In total	478	291	769
Annual average	48	29	77
%	62,16	37,84	100,00

Based on the available data of the Republic Institute of Statistics, in the period from 2012 to 2021, 769 fires occurred in state forests (table 1). In the total number of fires in state forests, ground fires account for 62.16% and tall fires for 37.84%. The highest number of fires was recorded in 2012, when 282 cases of forest fires were recorded. In the same year, the highest number of ground forest fires occurred on an annual basis in the observed period (211 cases). The lowest number of fires occurred in 2014, when only 12 cases of fires were recorded, of which 9 were ground fires and 3 high fires. The largest number of high fires occurred in 2018, as many as 174 cases.

Table 2: Total burned area and damaged wood mass (m³) in the forests of the Republic of Serbia in the period from 2012 to 2021(*Source: Authors*)

Year	Burned surface (ha)	Damaged wood mass (m ³)	Number of fires
2012	7.460	63.118	282
2013	561	7.343	43
2014	284	10.256	12
2015	827	5.059	47
2016	296	37.114	30
2017	1002	11.415	69
2018	303	707	185
2019	1.079	3.397	41
2020	196	5.147	26

Year	Burned surface (ha)	Damaged wood mass (m ³)	Number of fires
2021	834	10.099	34
In total	12.842	153.655	769
Annual average	1284	15.366	77

In order to adequately assess the damage caused as a result of forest fires in the observed period, it is necessary to take into account the data on the total area of the land that was affected by the fire (burnt area) as well as the total damaged volume of wood mass (table 2).

The total burned area in the forests of the Republic of Serbia in the period from 2012 to 2021 was 12,842 ha. The smallest burned area in the relevant period was recorded in 2020 and was 196 ha. The largest burned area is 7,460 ha and was recorded in 2012. The second significant year in terms of burned area is 2019, in which 41 fires engulfed as much as 1,079 ha of forest land and forests. The biggest difference between the number of fires and the burned surface area was observed in 2018, when 185 recorded fires caused damage to 303 ha of surface area.

The total volume of damaged timber in the state forests of Serbia in the period from 2012 to 2021 was 153,655 m³. The smallest damaged volume of wood mass in the observed period was recorded in 2018. The most damaged volume of wood mass was recorded in 2012, when 63,118 m³ of wood mass was destroyed.

3. CLIMATE CHANGES

The Intergovernmental Panel on Climate Change – IPCC defines climate change as the greatest global environmental problem of modern civilization which, if appropriate and urgent measures are not taken, may result in a further increase in air temperature between 1.4°S and 5.8°S by the end of the 21st century compared to 1990. year.

According to reports from 2007, it is stated that there has been an increase in the global average temperature, as well as that the impact of climate change will increase in the coming period, which will increase the number of extreme weather events. Various products of human work that have led to an increase in the concentration of certain gases in the atmosphere result in the appearance of the greenhouse effect and lead to an increase in the average annual temperature at the global level (Contribution of Working Group II to the Fourth Assessment Report of the IPCC).

The global mean temperature in 2022 was 1.15 [1.02 to 1.28] °C above the pre-industrial period (1850-1900). The six datasets used by WMO in the analysis are shown in figure 1 and place 2022 as the fifth or sixth warmest year globally (WMO, 2023).

According to the report of the World Meteorological Organization – WMO from 2022, the concentrations of the three main greenhouse gases (carbon dioxide, methane and nitrogen oxide) reached record values in 2021. Real-time data from specific locations shows that levels of the three gases will continue to increase in the future.

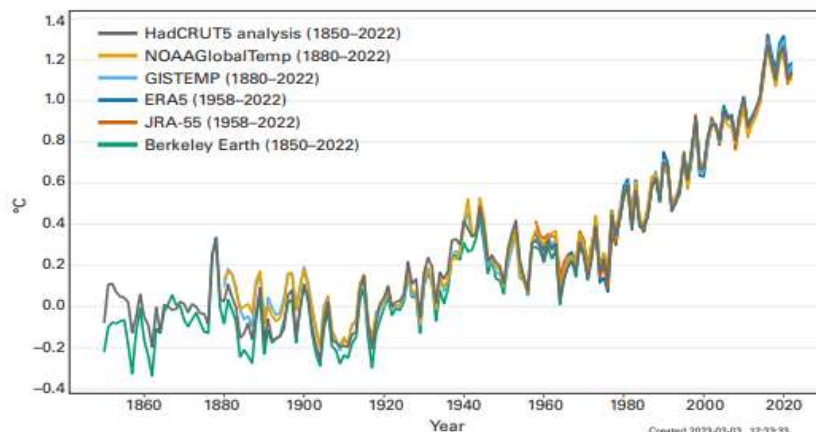


Figure 1. The global mean temperature
Source: WMO – State of the Global Climate 2022

The climate of Serbia can be described as moderate-continental with more or less pronounced local characteristics. Spatial distribution of climate parameters is determined by geographical location, relief and local influence, as a result of a combination of relief, air pressure distribution on a larger scale, terrain exposure, presence of river systems, vegetation, urbanization, etc (RHMZ Republic of Serbia).

3.1. Temperature and precipitation regime in Serbia

The temperature regime as a measure of thermal conditions in the territory of Serbia is primarily conditioned by solar radiation, geographical position and relief. Also, depending on the relief and exposure of the slopes, we have local climate characteristics everywhere in our country RHMZ Republic of Serbia).

The Republic Hydrometeorological Institute of Serbia announced on 18.01.2023. annual newsletter for Republic Serbia for 2022. According to him, the year 2022, with an average air temperature of 12.1°C, is the second warmest year (Figure 2) in the period from 1951 to the present day.

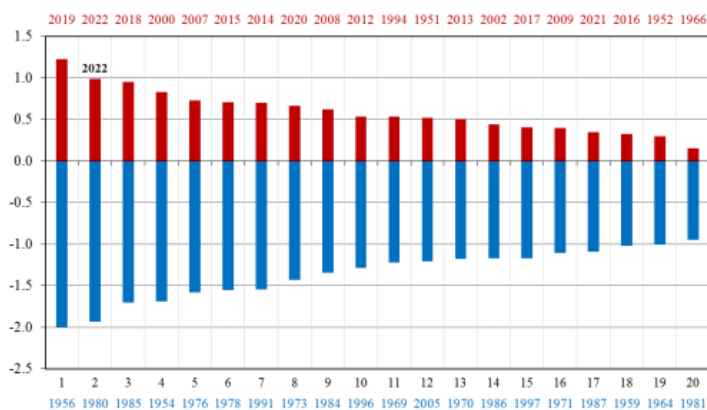


Figure 2. Ranking of the warmest and coldest years in the Republic of Serbia
Source: RHMZ of Serbia - Annual bulletin for Serbia for the year 2022

The annual temperature after 1980 tends to increase, that is, positive deviations in temperature are more frequent and their intensity increases. The last 10 years are ranked among the 15 warmest years (figure 2).

The highest daily air temperature during 2022 was measured on July 23 in Smederevska Palanka and was 40.6°C. In Negotin and Sombor, 2022 is the warmest year since the beginning of measurements at those stations. In most of Serbia, 40 to 70 tropical days were recorded, which is 5 to 26 tropical days more than the average number for the reference period 1991-2020. 40 tropical nights were registered in Belgrade, 14 nights more than the average.

According to the analysis of the summer season of 2022 for Serbia, the summer of 2022 is the third hottest summer in Serbia for the period of meteorological measurements from 1951 to 2022, and the hottest was in 2012 (RHMZ Republic of Serbia).

Precipitation is one of the most important climatic elements. Due to the atmospheric processes and features of the relief, precipitation is irregularly distributed in time and space on the territory of Serbia. The normal annual amount of precipitation for the whole country is 896 mm. Annual amounts of precipitation on average increase with altitude.



Figure 3: Normalized deviations of annual volumes. precipitation in Serbia period from 1950 to 2015

Source: RHMZ of Serbia

Looking at Figure 3, we can conclude that in the period from 1950 to 1981 in the Republic of Serbia, in most cases, the annual amount of precipitation is in accordance with the average or within normal limits. Exceptions were the rainy years 1954, 1955, and 1970, while 1953 and 1961 were moderately dry. After 1981, there are negative deviations, more precisely, the intensity of droughts increased. 1990, 1993 stand out as very dry years on an annual level and 2000 with an extremely severe drought. The years 2001, 2004 and 2005 stand out as rainy years in Serbia, while 2014 is presented as extremely rainy (Popovic et al., 2005).

According to the annual bulletin for the year 2022, in most of Serbia, the annual amount of precipitation was within the limits of the average, and in the west and in the part of eastern Serbia below the average. In Valjevo, 2022 is the second driest year, and in Požega the fourth driest in the past 97 years (RHMZ Republic of Serbia).

4. NEGATIVE INFLUENCE OF CLIMATE CHANGES ON FOREST FIRES

In the Republic of Serbia, forest fires are among the most frequent natural disasters. It has already been noted that the intensity and duration of the drought has increased, as a result of the increase in temperature, the decrease in summer precipitation and a greater number of longer dry periods, which favor the occurrence and development of forest fires and represent a constant threat to the loss of forests and forest land (Zivkovic, 2018).

According to the statistical data of the Republic Institute for Statistics in state forests, in the period 2012-2021. in Serbia, 769 forest fires were registered in state forests, on an area of 12,842 ha.

From the attached pictures and tables in the previous chapters, it can be seen that the largest number of fires were registered in 2012 and 2018, as well as that 2018 is the third warmest year for the period of meteorological measurements from 1951 to 2022 (Figure 2). And if the year 2012 is "only" in tenth place, it is even more characteristic that the summer of 2012 was declared the hottest summer in the Republic of Serbia for the period of meteorological measurements from 1951 to 2022. The lowest number of forest fires was recorded in 2014, only 12, and according to the data of RHMZ of Serbia, 2014 was the rainiest year in the period from 1951 to the present day (Figure 3).

From the aforementioned analysis, it is clearly observed that changes in the thermal and precipitation regime have a great influence on the occurrence of forest fires.

5. PREVENTION OF FOREST FIRES

The basic tasks of forest fire protection are: forecasting the danger of fire, early detection of fires and their rapid localization and extinguishing.

Various researches have come to the conclusion that humans are the most common cause of fires, so effective measures to prevent fires would be raising the level of public awareness of the ecological, economic, social and cultural importance of forests, appealing to the increased risk of forest fires, placing prohibition signs and signs warnings at approaches to the forest, next to roads, picnic areas, tourist facilities;

The guard service should control the potential causers of forest fires, that is, farmers who burn stubble after harvest, weeds and other plant material, owners of weekend facilities, collectors of forest fruits, medicinal plants and mushrooms, hikers, visitors;

A forest fire can break out in very inaccessible terrain, it is difficult to spot it in time, report it and start extinguishing it. It is very important to quickly detect the occurrence of a fire, and it can be ensured by monitoring endangered forests and by introducing on-calls in critical periods of forest fires. After detection, it is necessary to ensure a quick response, i.e. extinguishing forest fires. A developed road network is needed, especially according to the areas that are most at risk, mobility and equipment of teams for quickly extinguishing forest fires, organized water intakes and water accumulations, maintenance and arrangement of water sources in forests with the obligation to preserve habitats with water sources; training and improvement of workers in the field of forest fire protection.

6. CONCLUSION

If we look at the causes of forest fires, we will easily conclude that prevention is key. In most cases, man is considered the main "culprit", through his direct action due to carelessness and negligence or indirectly through negative impact on the atmosphere and climate change..

A forest fire is an uncontrolled, spontaneous movement of fire across the forest surface and represents one of the most destructive natural forces. In our country, outdoor fires are one of the most frequent natural disasters. Depending on the type of fire, the form and speed of its spread, the configuration of the terrain on which it occurs and the existing climatic conditions, the type of fire varies, as well as the amount of damage it can cause.

The analysis of meteorological data indicates that the annual temperature has been continuously increasing in recent years and decades, and that there are oscillations in precipitation with more frequent occurrence of deficits. These two most important climate

elements show that we are greatly witnessing climate change and that the increase in global temperature is becoming an increasingly serious problem.

It seems that forest fires will become a common occurrence for most countries in the future. Accordingly, it is necessary to strengthen resilience at the national level, enable integrated disaster risk management, but also ensure a sufficient number of resources and means to fight emergency situations of this nature.

In the Republic of Serbia, the reform of the management system in emergency situations began in 2009, when the Department for Emergency Situations was formed, and it needs to be continued. It would be of great importance to continuously educate the widest population, through educational activities, information about dangers and their consequences. Also, the tightening of legal regulations would certainly affect the awareness of citizens and further reduce the risks of fire.

REFERENCES

Aleksic, P. Krstic, M. Jancic, G. (2009), Forest fires-ecological and economic problem in Serbia. *Botanica Serbica*. 33 (2): 169-176 (2009)

Aleksic, P. Jancic, G. (2011), Zastita suma od sumskih pozara u Javnom preduzeću „Srbijasume”, *Sumarstvo*, broj 1-2, str. 95-110, Beograd

Avramovic, D. Mihajlovic, E. Ilic-Petkovic, A. Milosevic, L. (2017), Pokazatelji stanja sumskih pozara u drzavnim sumama Srbije u periodu od 2007. do 2016. godine, *Zastita na radu – Put uspesnog poslovanja*, 14. Medjunarodna konferencija Divcibare, str. 214-222

Ministarstvo unutarasnjih poslova (2017), *Assessment of the risk of disasters in the Republic of Serbia 2017*, Beograd

Popovic, T. Radulovic, E. Jovanovic, M. (2005), Kolikonam se menja klima, kakva ce biti nasa buduca klima?, *Zivotna sredina ka Evropi*, Agencija za zastitu zivotne sredine, Beograd

Republički hidrometeorološki zavod Srbije (2023), *Godisnji bilten za Srbiju za 2022. godinu*, Beograd

Republički hidrometeorološki zavod Srbije (2022). *Sezonski bilten za Srbiju leto 2022. godine*, Beograd

Republički zavod za statistiku, *Pokazatelji stanja sumskih pozara u drzavnim sumama Srbije u periodu od 2012-2021. godine*

Zakon o zastiti od pozara – ("Sl. Glasnik RS", br. 111/2009, 20/2015, 87/2018, 87/2018 – dr. zakoni)

Zivkovic J. (2018), *Uticaj sumskih pozara na prirodne ekosisteme oblasti visok*, Univerzitet u Nisu, Fakultet zastite na radu u Nisu, magistarska teza, Nis

<https://www.ipcc.ch/> , Accessed: 17.08. 2023.

<https://public.wmo.int/en>, Accessed: 20.08.2023.

RESPONSE OF THE ARMY OF SERBIA TO NON- MILITARY THREAT - MIGRATION

Nikola Banjac¹, Nenad Komazec^{2a}

¹ Ministry of Defense, Bircaninova 5, Belgrade, Republic of Serbia, banjajn@gmail.com

² University of Defence in Belgrade, Military Academy, Veljka Lukica-Kurjaka
33, Belgrade, Republic of Serbia, nenadkomazec@yahoo.com

Received: 15th August 2023

Accepted: 4th September 2023

Review paper

Abstract: *The issue of work indicates that with the global connection of the world or more precisely with the opening of borders, easier access, development of technologies, migrations are becoming more frequent, one could say almost an everyday occurrence. The main security risk is still the possibility of radical Islamists and returnee fighters from the Middle East infiltrating among migrants entering the Republic of Bulgaria and Macedonia. Serbia. Migrant smuggling activities remain the biggest security threat.*

The research in the work raises an issue that needs to be further analyzed, bearing in mind the fact that the migration crisis is becoming more complicated and requires new responses and forms of organization and protection of the country, and is reflected in the fact that the external factors of migration deserve special research in order to identify security risks and threats. overview and assessment of the policies of countries in the surrounding area, and above all the views of the key actors of the EU, with an emphasis on the impact and consequences for the Republic of Serbia, as well as predicting possible directions of development of the migrant crisis and preventive actions of the Republic of Serbia to protect national interests.

Key words: *security, national interests, migration, laws, Republic of Serbia*

1. INTRODUCTION

According to some analysts, this is not a „refugee crisis”, this is a migration of people. The scale of migration is biblical. The waves of „migrants” include, first of all, young, adult men of military age, who left the hearth, wives, children and elderly parents and left them at the mercy of life. Apparently, it makes us think that among the many migrants (refugees) there are also military deserters. So, here, among other things, we are dealing with deserters, among whom numerous security services have discovered a large number of terrorists. We see more and more that they are well organized, have maps with movement routes, are solidly dressed, have expensive and modern „smart mobile phones”, withdraw money in banks in an organized manner, etc. Social differences among migrants are recognizable. We have witnessed that, if

^a ORCID: 0000-0001-9227-118X

the host countries do not tolerate their usual, diverse, even aggressive and demanding behavior, they become partially violent and prone to various forms of socially unacceptable behavior.

In the event that the EU completely „walls off” the Balkans, which seems to be a question of „when” rather than „if”, tens of thousands of disaffected people will find themselves stuck in a country they never wanted to stay in and in the midst of a society that does not want them, but is forced to take care of them. Looking at the scandals in Slovenia, on the border between Serbia and Hungary at Horgos, as well as indicators of the likely outcome when migrants become upset about their living conditions, they can burn down their settlements as they have been doing. It is very difficult to control large groups of people. . Whether or not migrants will socialize into the environment they came to remains a problem. Deeply dissatisfied with the fact that they are forced to live in a country they do not want to live in, not because of the people who live there, but because of the wrong expectations of most of them who assumed that they can achieve their goals and desires (Radisic, 2017).

As a result of the lack of a unified position on the migrant crisis within the European Union, which puts peripheral countries in the position of the first entry country, and the reactions of individual states that were on the migrant route (erecting fences, closing borders), there was a temporary disruption of interstate relations between: Serbia- Hungary, Serbia-Croatia, Croatia with Hungary and Slovenia, as well as Greece with Macedonia. After which, with the intensification of cooperation between the mentioned countries, relations became more relaxed on the mentioned issue. However, bearing in mind the permanent commitments of the aforementioned countries regarding the reception of migrants, the allocation of funds, their retention in their territory and the granting of asylum, in the long term we can expect the re-closing of the borders, which will have a direct impact on the security of the Republic of Serbia, through an increase in the number of migrants and the time they are detained on the territory of R. Serbia.

2. CONSEQUENCES OF THE MIGRANT CRISIS FOR NATIONAL SECURITY

In the Republic of Serbia, several strategic documents concerning migration management have been adopted for the purpose of solving certain issues. The Republic of Serbia is a signatory to the Geneva Convention from 1951 and the Protocol from 1967, as well as a number of international documents that are important in the field of migration management. The highest legal act of the state, the Constitution from 2006, contains several articles that are important for the area of migration management. Article 13 of the Constitution refers to the protection of our citizens abroad. Article 17 of the Constitution deals with the position of foreigners, it stipulates that foreigners, in accordance with international agreements, have in the Republic of Serbia all the rights guaranteed by the Constitution and the law, with the exception of the rights that according to the Constitution and the law belong exclusively to the citizens of the Republic of Serbia. In the part of the Constitution that deals with human and minority rights and freedoms, there are a number of provisions that are important for different categories of migrants. The immediate application of human and minority rights guaranteed by the Constitution (Article 18) is foreseen, as well as the prohibition of discrimination (Article 21). Before the Constitution and the law, everyone is equal and everyone has the right to equal legal protection, without discrimination (Constitution of RS).

The wider inclusion of the issue of population migration in national strategies and laws was due to the necessity of transformation and adaptation to European documents, all because of accession negotiations on membership in the European Union. The Asylum Law adopted in 2007 was the first law of its kind in the country's legal system. With its adoption, Serbia undertook to help and protect all asylum seekers on its territory. However, it was necessary to

supplement the law and introduce the necessary changes in accordance with the large influx of migrants since 2015. Thus, in March 2018, the new Law on Asylum and Temporary Protection was adopted, whereby the state harmonizes its legislation with the legal acquires of the European Union and strives to make the asylum procedure more efficient. At the same time, the Law on Foreigners was adopted, which better defines the rights and obligations of foreigners in the Republic of Serbia (Law on Foreigners of the Republic of Serbia).

The national framework for migration management is represented by existing legal and institutional frameworks. After assessing the situation and expected trends, priority activities are determined, which are reflected in the adoption of the appropriate legal framework and the implementation of relevant strategies. In Serbia, they refer to: Law on Travel Documents (2007), Law on State Border Protection (2008), Strategy (2009), and then the Law on Migration Management (2012), Strategy for Combating Illegal Migration in the Republic of Serbia in the period from 2009 to 2014, Strategy for combating irregular migration in the Republic of Serbia for the period from 2018 to 2020 (2018), Strategy for Combating Human Trafficking in the Republic of Serbia (2006), Strategy for Integrated Border Management and others. The establishment of the Coordinating Body for Monitoring and Management of Migration in 2009 is also significant. These legal frameworks were further operationalized through strategic documents and rules related to migration management and the system of reception and accommodation of asylum seekers.

In addition to the existence of a legislative framework, it was very important in the conditions of the influx of a large number of migrants on the territory of Serbia to establish a working body that would deal with specific issues and problems on the ground. Thus, already in June 2015, the Government of the Republic of Serbia established the "Working Group for Solving the Problem of Mixed Migration Flows", consisting of five ministries: the Ministry of the Interior, the Ministry of Labor, Employment, Veterans and Social Affairs, the Ministry of Health, the Ministry of European integration, Ministry of Foreign Affairs. In addition, the Commissariat for Refugees and Migration and the Delegation of the European Union in Serbia are also members. The task of the Working Group is to monitor, analyze and discuss the issues of mixed migration flows in the Republic of Serbia with special reference to the problems in this area, provide analyzes of the situation and proposals for measures to solve the observed problems and harmonize the views of the competent state authorities and other organizations and institutions that deal with the issue of mixed migration flows (Working Group Decision).

Also, the members of this group are responsible for the coordination and cooperation of various organizations that deal with this issue in establishing adequate reception and transit conditions, strengthening the system for registering migrants, and in providing key services, which include reception, accommodation, health care, food and other products, water and sanitary conditions. (www.kirs.gov.rs) In accordance with the provisions on the functioning of the Working Group and its primary tasks, a large number of international organizations, primarily the International Organization for Migration (IOM), the UN High Commissioner for Refugees (UNHCR), but also numerous civil society organizations, are involved in helping migrants, but in consultation with the Working Group. In addition to their presence in reception centers, depending on the current situation on the route, these organizations also provided assistance to migrants at border crossings, in informal camps, that is, where certain persons found themselves in larger numbers. Their task was to provide migrants with information about the possibilities of obtaining asylum in the Republic of Serbia, to inform them about medical assistance, translators, as well as to provide them with psycho-social support. Also, they work with children including them in various activities in the centers and help them with their schoolwork, work with individuals with special needs, with unaccompanied minors, assist in voluntary return and provide them with transportation, food, water and other necessary things.

Government R. Serbia, in coordination with international and non-governmental organizations, organized the provision of humanitarian aid at the border entry and exit points of the migrant route as an emergency measure to the growing problem of the influx of migrants. The method of work of state authorities on registration and issuing documents to migrants for free movement through the territory of the Republic of Croatia has been established. Serbia. The process of registering migrants was carried out based on the provisions of the Asylum Act. (Act on Azir) In addition to the already existing asylum centers in Banja Koviljaca, Bogovodja, Obrenovac, Tutin, Sjenica, Krnjaca (until the former military facility in Mladenovac was put into operation), new Reception and Transit Centers were opened with functions of accommodation and acceptance of migrants in Presevo, Subotica, Sida, Dimitrovgrad and Bujanovac (<http://www.kirs.gov.rs>). Potential locations for opening additional centers in case of an increase in the number of migrants and refugees, which exceeds the available accommodation.

In accordance with the increase in the number of migrants in 2015, temporary centers were opened in the north and west of the country, and after the closure of the route and the significantly longer detention of migrants in Serbia (up to two years), new ones were opened. In addition to these activities in providing the basic conditions for the reception of migrants on the Balkan route, the Working Group had a series of bilateral meetings with representatives of international organizations, ambassadors, donors, in order to improve the conditions in the centers for the reception of migrants, and to expand the capacities in accordance with the needs.

An important body for advisory work related to migration management on the territory of the autonomous province, as well as local self-governments, is the provincial or local Council for Migration. Its work is defined in the Migration Management Strategy from 2009. The Council is obliged to monitor and report to the Commissariat for Refugees and Migration on migration in the province, that is, on the territory of a certain local self-government. It is necessary to propose measures and plans of activities that should be undertaken in order to effectively manage migration in a certain territory. The work of the council at local levels also deals with the problem of irregular migration in the municipalities where the reception centers are located, as well as the border municipalities, through which migrants move in attempts to reach the territory of the European Union.

Another significant response of the institutions to the so-called the migrant crisis is also the state's decision to include migrant children in the education system. By ratifying the UN Convention on the Rights of the Child, the Republic of Serbia undertook to ensure the realization of all children's rights. Through the cooperation program of UNICEF and the Government of the Republic of Serbia in the field of education in the period 2016-2017. In 2008, the Joint Concept of Supporting the Education of Migrant Children and the Project Supporting the Education of Migrant Students in the Republic of Serbia were implemented.

The Republic of Serbia, due to its position, suffers one of the greatest pressures of irregular migration, because some of the key transit routes lead through our territory. The largest number of migrants to Serbia still comes from the direction of North Macedonia and the Republic of Bulgaria. According to the latest data from the Republic's Commissariat for Refugees and Migration, 16 reception and asylum centers for refugees and migrants, which is four less than in the state of emergency, because the number of migrants in the country is also lower, and 4,882 people are accommodated in those centers. According to the national structure, the most migrants are from Afghanistan, 39 percent, followed by Syria 19, Bangladesh 12, Pakistan seven percent and Iran five percent. Also, according to the Commissariat for Refugees and Migration, since the beginning of the corona virus epidemic, there have been no positive cases

among refugees and migrants. During the state of emergency, 27 people suspected of the corona virus were tested and all were negative.

In connection with the current situation with the corona virus pandemic, the Commissariat for Refugees and Migration states that since the beginning of July 2020 and the latest data indicating an increase in the number of people suffering from COVID-19 in Serbia, the enhanced hygiene regime has started to return to the centers again and other recommended epidemiological protection measures. This means that migrants are also involved in increased cleaning, airing of rooms, disinfection, that protective masks and disinfectants are provided, and that they are informed about the situation with the pandemic every day, through a daily bulletin in their languages, which is sent to them, printed and distributed. In the world and in Serbia, as well as with all measures taken by the state to suppress the infection.

Since the beginning of 2020, 1,277 persons have expressed their intention to request asylum, while only 50 of them have actually submitted a request and they are in our asylum centers. This information tells us that they do not want to stay in the Republic of Serbia, but use it only as an administrative mechanism to continue their journey to Western Europe. Serbia continues to be a constructive partner in the complex migrant problem, but we certainly need to continue insisting that we cannot be a country that will only become a country waiting for asylum applications to be processed, nor a country for the return of migrants who used the route through the Western Balkans. As for the smuggling of migrants, the fight of the Serbian police in that area is still very intense. In the first half of 2020 alone, 90 criminal charges were filed against 104 people on suspicion of having committed this crime and also 5 criminal charges against organized criminal groups consisting of 25 members. These figures compared to data from 2018 and 2019 show a certain increase in this incriminating activity, but also success in detecting and prosecuting perpetrators.

At the time of the declaration of a state of emergency on the territory of the Republic of Serbia, due to the epidemic of COVID-19, about 5,900 migrants were accommodated in centers for the accommodation of asylum seekers and reception centers. With the declaration of a state of emergency, accommodation facilities became too small to provide accommodation for all who needed it. That is why new facilities were opened, namely temporary centers in Miratovac and Morovic.

At the beginning of May 2020, after the end of the state of emergency, there were slightly more than 9,500 migrants in reception centers throughout the Republic of Serbia. It can be said that the migrants patiently and responsibly shared the fate of the citizens of Serbia. Thanks to the great efforts of all actors and institutions involved in migration management, no cases of infection with the new virus were recorded among the migrant population during that period.

In the migration management process, Serbia continues to act in a responsible, organized and humane manner, making maximum efforts to, as much as possible in the conditions of the pandemic and the greater influx of migrants to the centers, meet the standards in the area of acceptance, care, accommodation, legal, social and health protection of migrants which are located in its territory.

3. THE RESPONSE OF THE SERBIAN ARMED FORCES TO NON-MILITARY THREATS - MIGRATION

Due to its social importance and the role it plays in the defense system, the army is traditionally an integral part of the constitutional matter. Many states already regulate its position and basic competence in the national defense system in the constitutional provisions. In this way, the highest legal act defines the social reason for the existence of the army, which can be seen from those constitutional norms that determine the social values that it must protect. In the

most general sense, these are the social values for which the defense system is established and which also determine its basic social function (Markovic, 2010).

The Constitution of the Republic of Serbia regulates the basic function of the armed forces. According to this act, their main task is to defend the state against armed threats from the outside and to carry out other missions and tasks in accordance with the Constitution, the law and the principles of international law that regulate the use of force. It is not clear from this provision what values it defends, but it can be seen from the provision that places the regulation and provision of sovereignty, territorial integrity and security of the state under the jurisdiction of the Republic of Serbia (Constitution of RS).

The primary function of the armed forces is to defend the sovereignty, independence and territorial integrity of the state. This is their traditional function, which determines their existence. In constitutional practice, some other social values are mentioned, the defense of which is the responsibility of the armed forces, but even so, the function of the armed forces is primarily conditioned by an external factor that threatens the security of the state. In other words, the armed forces exist to protect the stated values when they are threatened by armed means from the outside, that is, by aggression. In addition, their existence aims to deter aggression, which also defines their function.

Similar provisions on the armed forces found in the Constitution of the Republic of Serbia can be found in the constitutional provisions of other countries. For example, the Constitution of Austria states that the federal army protects constitutional institutions and democratic freedoms, internal order and security of the state, provides assistance to civil structures in cases of natural disasters and large-scale accidents. (Constitution of Austria) According to the provisions of the Polish Constitution, the function of the armed forces is defense of independence, territorial integrity and inviolability of state borders. (Constitution of Poland) The Armed Forces of Romania are exclusively in the interest of the people of guaranteeing the sovereignty, independence and unity of the state, territorial integrity and constitutional democracy. Larger scale or acts of terrorism in circumstances where the security authorities are unable to act independently.

In addition to the above, we must not forget the cases of technical-technological and natural disasters, when the armed forces provide assistance to the institutions of civil authority. Generally speaking, these are situations that, in accordance with the regulations on defense, are considered a reason for declaring a state of emergency, i.e. an emergency situation. Many countries regulate this function of the armed forces with constitutional or legal regulations that regulate the field of defense. The function in question is not primary but secondary because it is realized only when other competent state bodies are not able to independently oppose such phenomena. The armed forces of Hungary can also be used in the event of an armed action directed against the constitutional order, the seizure of power or in the event of critical acts of armed violence that seriously endanger the lives and property of citizens on a mass scale if the use of the police proves to be insufficient as in the case of natural and industrial disasters (Constitution of Hungary). In addition, the armed forces of Germany can be engaged to support the police forces if a natural disaster or accident threatens more than the territory of one federal state. In addition, and in order to defend against a threat to the survival of the state or to defend the free democratic basic order of the federal state or a country, the federal government can use the armed forces in support of the police and federal border protection and in order to protect civilian objects and in the fight against organized and armed uprising (Constitution of the Federal Republic of Germany).

In accordance with the aforementioned practice, units of the Serbian Armed Forces can be engaged in providing assistance to the population, in the event of natural and other large-scale

disasters in which the lives and health of people and animals and their material goods are threatened in a certain territory, and based on the request of the competent authorities for the protection and rescue of people and material goods. In such circumstances, the Chief of the General Staff of the Serbian Armed Forces, i.e. the head of the competent command, and in order to protect and save people, material and cultural assets from natural disasters, technical-technological accidents and disasters, the consequences of terrorism and other major accidents, can order measures to implement preparedness and use parts of the Serbian Armed Forces in order to eliminate the harmful consequences that may arise from non-military threats to security (RS Defense Law).

As an armed force, the Serbian Armed Forces play a very important role in the defense system of the Republic of Serbia, because with its organization, equipment, operational and other capabilities, it represents a deterrent against all forms of threats to the security of the Republic of Serbia. The missions and tasks of the Army are determined by the Defense Strategy in accordance with the Constitution and based on the inalienable right of the Republic of Serbia to individual and collective defense, in accordance with Article 51 of the UN Charter and the basic principles of international law (Defense Strategy of the RS).

In conditions of increasing challenges, risks and threats to security, as well as possible military and non-military threats to the security of the Republic of Serbia, the Serbian Armed Forces can engage in a wide range of operations, which requires it to build operational capabilities that can respond to its missions. From the aspect of preventing illegal migration, the tasks from the third mission are particularly significant, and the main focus is the participation of units of the Serbian Army in securing the state border, in order to prevent illegal crossings of migrants and control the territory of the Republic of Serbia.

In addition to the above, the Law on Defense as a general systemic legal act also stipulates the obligation of cooperation between the Army and the Police in cases where the border zone, the border, and the lives of people and material goods in that area are threatened. In these circumstances, the Government, at the joint proposal of the Minister of Interior and Defense and with the consent of the President of the Republic, forms a joint military-police force. (Law on the Defense of the RS)

Due to the migration crisis at the end of 2015 and the beginning of 2016, the Ministry of Internal Affairs and the Border Police Directorate additionally strengthened the capacities for securing the state border. However, the engaged capacities were not able to adequately respond to the newly created situation. The new situation on the ground and the increasing influx of migrants required a quick response and engagement of the capacities of the Serbian Armed Forces. When it comes to the engagement of members of the Serbian Armed Forces, they became involved in solving the problem of the increased influx of migrants in the second half of June 2015. In the initial period, they participated in the organization of the reception of migrants at the border with the Republic of Macedonia on the tasks of arranging reception centers, health care, water supply, hygienic bathing and temporary accommodation of migrants. However, further complicating the situation (at the beginning of 2016), Military Police units were also included in the implementation of the tasks, with the basic mission of securing the state border in the regular security system, with the aim of preventing illegal crossings of migrants and controlling the territory of the Republic of Serbia.

During that time, it was registered that around 9,700 migrants were prevented from crossing, and 145 smugglers were detained and prosecuted. When the state borders with Macedonia and Bulgaria were closed, a new direction through the Raska-Polim area was also registered, so their operation was extended to another sector, which includes part of the administrative line and part of the state border with Montenegro (Miljic, 2017).

In accordance with a specific mission, Joint Forces were formed from units of the Serbian Armed Forces and the Ministry of Internal Affairs of the Republic of Serbia. From the beginning, the engagement of joint forces was set up as joint and mixed, from the level of the command of the Joint Forces, all the way to the authorities in space. The commander of each body in the area is a military officer, and in the body, depending on its purpose, whether it is for line or depth security. In addition to members of the Army, members of the border police, police intervention units, traffic police and gendarmerie were also engaged, i.e. the holders of authorizations for migrants or smugglers, while the military part of the engaged bodies had the task of assisting the holders of authorizations. After receiving the task of forming the Joint Forces, drawing up Plans and deploying units, the Joint Forces Command was formed in the second half of July 2016. In addition to members of the Serbian Armed Forces and the Ministry of Internal Affairs, the Joint Forces Command also includes members of the security services (BIA, VBA and VOA), the Ministry of Labour, Employment, Veterans and Social Affairs and the Commissariat for Refugees and Migration. In the initial period, the primary task was to observe and assess the situation with regard to the movement of migrants in order to determine the adequate distribution of units along the border line (Simovic, 2017).

The task was carried out by a combination of line and depth security in regular mode. Line security was carried out from the former checkpoints through control of the border line through patrolling, observation, deployment of regional guards, observation posts and ambushes. For in-depth security, forces are deployed in the depth of the territory, where traffic control points, patrols, observation posts and ambushes are organized, along with constant control of road and rail traffic. . Plans have been drawn up for measures to be taken in the event of attempts at mass illegal crossings of the state border. The engagement of helicopter units of the Army and the Police was carried out very restrictively, mainly for reconnaissance of certain regions and directions in order to collect the necessary data. The zone of engagement included the area along the border with Bulgaria and Macedonia, and from mid-December 2016, a part of the area within the scope of the border with Montenegro, so that the total length was 560 kilometers.

In the initial period of engagement of joint forces, the greatest pressure to enter Serbia came from Macedonia, and later the number of illegal crossings of the state border from Bulgaria increased considerably. The largest number of migrants was from Afghanistan. Most of the migrants from Pakistan were Afghan refugees of Pashtun nationality. Migrants from Syria and Iraq were with their families, which is not the case with Afghans who are very young and mostly male. Migrants from Syria and Iraq mostly came from the direction of Macedonia, and migrants from Afghanistan from the direction of Bulgaria. From the other countries, Cuba, Bangladesh, Sri Lanka, Uganda, Rwanda and Eritrea, there were very few illegal crossings compared to the ones listed.

In addition to the engaged forces of the Republic of Serbia, 220 international police officers were also engaged, as a form of additional forces from the European Union (from Hungary, the Czech Republic and Slovakia) (Simovic, 2017). These EU forces were engaged in areas where the risk analysis determined that is the most threatened border, that is, where the pressure and influx of migrants is greatest. On that occasion, the members of the international forces were familiarized with our legislation and the competences and powers of the border police and the Joint Forces, and at the same time with their rights and obligations. The effects of such measures are a reduced number of migrants since the beginning of 2017, a change in the routes of movement and smuggling of migrants, which was confirmed during the exchange of information between all security services, both in the Republic of Serbia and in the region.

Certainly, the Ministry of Internal Affairs, in accordance with its capacities, made a great contribution to the current migrant crisis, however, with the involvement of the Serbian Army in the implementation of this task, that effect was significantly increased. Even more significant is the joint engagement of the Serbian Army and the Ministry of Interior in response to security challenges, risks and security threats.

The action of the Joint Forces towards the Republic of Macedonia and Bulgaria had extraordinary effects. About 20,000 illegal migrants were discovered, of which about 19,000 were prevented from crossing the territory of the Republic of Serbia. In addition to the above, about 2,000 smuggled persons were discovered and placed in reception centers. The engagement of joint forces contributed to the fact that several tens of thousands of migrants changed their decision to go through the Republic of Serbia, that is, they chose other routes to transfer to Western Europe, which is particularly important in the readmission process.

Effective engagement of the Joint Forces towards the Republic of Bulgaria and Macedonia significantly reduced the number of illegal border crossings. This led to the opening of a new alternative route through Montenegro, so from December 2016, the engagement of the Joint Forces also began on part of the border with this neighboring country. (Milic, 2017) Based on the data so far, the conclusion is that a small number of migrants choose that route, however, the possibility that the number will increase on that route is not excluded, especially if the situation in Turkey becomes more complicated. . When considering the number of challenges that members of the engaged forces face on the ground, the biggest challenge, besides migrants, is the fight against smugglers. This phenomenon is very widespread and brings great material profit.

In addition to the above, until the disbandment in April 2018, the examples of the successful work of the Command of the Joint Forces of the Army and the Police speak of their professional and professional work, among other things, the successful action against the smuggling of migrants. Out of 172 smugglers, 134 are Serbian citizens, and 38 are foreign citizens. (Bulgaria 17, Pakistan 6, Iraq 6, Afghanistan 5, Moldova 1, Netherlands 1, BiH 1, and Austria 1). Over 80 passenger vehicles and over 50 vans were used in attempts to smuggle migrants. During the reforms and reduction in the number of members, the Army handed over the security of the state border to the Ministry of Internal Affairs and kept the only security of the administrative line towards Kosovo and Metohija, so it adapted the training of its members for this task. However, at the moment when it received the task of securing the border with Macedonia and Bulgaria, there were a sufficient number of senior officers in the Serbian Army who had experience in carrying out this task, and the military police units could immediately join the joint work with the forces of the MUP. What was a difficulty was the strain on the manpower, as well as the need to prepare certain accommodation capacities, since the Army abandoned the facilities it previously used for the tasks of securing the state border.

Inadequate equipment at the disposal of the Serbian Armed Forces (optoelectronic and thermal imaging devices) for monitoring the movement of migrants at night, as well as communication with migrants, which was mostly in English, represented a difficulty to a certain extent. A special question is whether the Joint Forces of the Army and the Police were engaged in a timely manner or with a delay. We saw that the force was formed in July 2016, when a decrease in the number of migrants arriving in Europe via the Eastern Mediterranean route was already recorded. For example, Hungary and Macedonia already engaged their armed forces in 2015 on tasks related to the migrant crisis, so it could be assumed that the use of the Serbian Armed Forces would be necessary. In this sense, it can be discussed whether it was too late to engage the Security Council, as well as whether it would be more rational to form a temporary composition, a special unit for this task.

How can the migrant crisis be repeated, especially if it is taken into account that the crisis in the Middle East and the security and economic situation in certain countries of North and East Africa, as well as the divergence between the EU and Turkey in terms of respect for human rights and freedoms, which can cause their mutual distrust and friction, it is important that the Serbian Armed Forces be ready for re-engagement at the border in order to prevent the uncontrolled entry of migrants into the territory of the Republic of Serbia.

In this regard, it is important that the Serbian Armed Forces ensure that the experiences of its members engaged in the previous period in various positions within the Joint Forces of the Army and the Police are entered into the system of lessons learned, systematized, translated into rules and introduced into the training system. Systematized and put into practice in this way, those experiences would not only be significant for the potential involvement of the Army in securing the state border, but also in carrying out tasks in multinational operations and providing assistance to local authorities in combating terrorism.

4. CONCLUSION

Although the Republic of Serbia has made maximum efforts to bring the process of migration through its territory under full control, the dangers that disturb its security have not been eliminated. Considering the non-uniform attitude of the members of the European Union, the permanent determination of certain neighboring countries regarding the reception of migrants, above all Hungary, it is to be expected that this problem will be in focus in the coming period as well, and therefore have a direct impact on the security of the Republic of Serbia. Primarily in the form of an increase in the number of migrants and their longer stay, i.e. staying in the territory.

Given that the Republic of Serbia is a candidate for membership in the European Union and that the process of accession negotiations has begun with the opening and harmonization of the necessary chapters, effective migration management is one of the conditions on which Serbia's accession to the European Union depends. The area of migration is legally and institutionally organized in accordance with the necessary standards of the European Union. The Government of the Republic of Serbia first arranged the legislative framework for the development of the migration management system. The legislative framework was developed on the platform of international law, and all ratified-confirmed international treaties, as well as all laws and other general acts, are in accordance with the Constitution of the Republic of Serbia.

A kind of *lock down* has become the generally accepted pattern of response of most European countries to the crisis caused by the COVID-19 pandemic, which inevitably resulted in a drastic reduction in the number of people in the, until then, continuous migrant columns. From the moment the measures were eased (from June until the autumn months of 2020, which were marked by a new increase in the number of new cases in Europe), the EU Border Protection Agency recorded an increase in migration compared to the „closure” period. So, generally speaking, the year 2020 was significantly different from the previous ones in terms of migration as well. In case of renewal of migration flows and total closure of borders by neighbors, there is a danger of creation of refugee camps-ghettos on the territory of the Republic of Serbia. In such an environment, the consequences of the migrant crisis for the security of the Republic of Serbia would be more complex and would require considerable efforts to eliminate them. Such a scenario imposes the need to consider and assess possible future consequences for the security of the Republic of Serbia and to make decisions in accordance with national interests.

In the coming period, the security situation may be complicated by the arrival of a larger number of "economic migrants", the return of a part of migrants from Western European countries to the Republic of Moldova. Serbia, bearing in mind the readmission agreement signed by R. Serbia and the possibility of Western European countries closing their borders. Such a situation and the absence of a clear European position on the status of migrants will increase the possibility of opening new security risks in Russia. Serbia, such as the increase in criminal activity, the possibility of causing incidents between migrants and the local population, the increase in xenophobia and Islamophobia among the local population.

The comprehensiveness and intensity of threats to the security of the Republic of Serbia caused by the migrant crisis requires a planned, coordinated and extensive response by all state entities, in order to minimize the impact of external factors on the threat to the national security system. bearing in mind that it is the obligation of all state bodies to work to protect the vital interests of the Republic of Serbia, this imposes the need to successfully control the migrant crisis, which as a necessity necessarily imposes the collection and exchange of reliable information, on the basis of which possible variants of the development of the migrant crisis will be analyzed and predicted crises, and act preventively based on them.

REFERENCES

- Asylum Law. (2007). Official Gazette of the Republic of Serbia, Belgrade,
- Miljic B. (2017). Balkan routes without roads, Defrana, magazine of the Ministry of Defense and the Serbian Army, no. 277, Belgrade
- Commissariat for Refugees and Migration of the Republic of Serbia, www.kirs.gov.rs
- Constitution of the Republic of Austria
<http://www.legislationonline.org/documents/section/constitutions>.
- Constitution of the Republic of Hungary,
<http://www.wipo.int/edocs/lexdocs/laws/en/hu/hu047en.pdf>. Constitution of the Federal
- Constitution of the Republic of Poland, <http://www.sejm.gov.pl/prawo/konst/angielski/konl.htm>.
- Constitution of the Republic of Romania,
http://www.cdep.ro/pls/dic/site.page?den=act2_2&parl=3#t3c5s1sball8
- Constitution of the Republic of Serbia. (2006). Official Gazette of the RS, Belgrade
- Constitution of the Republic of Serbia; Sl. Gazette of the RS, no. 98/2006. Adoption of new laws on asylum and foreigners (accessed 25 January 2021); <http://azil.rs/usvajanje-novih-zakona-o-azilu-i-strancima/>.
- Decision on the formation of a working group for solving the problem of mixed migration flows; Official Gazette of the RS, no. 54/2015
- Defense Strategy of the Republic of Serbia. (2019). Official Gazette of the RS, Belgrade
- Law on Defense of the RS, Official Gazette of the RS, no. 116/2007, 88/2009, 104/2009 and 10/2015
- Law on Migration Management. (2012). Official Gazette of the RS, Belgrade
- Markovic R. (2010). Constitutional Law, Faculty of Law, University of Belgrade. White City Republic of Germany, <http://www.btg-bestellservice.de/pdf/80201000.pdf>.
- Simovic M. (2017). Migrant crisis, Military work, no. 1, Defense Media Center. White City. <http://www.kirs.gov.rs/articles/navigate.php?type1=3&lang=SER&id=2682&date=>

PERCEPTION OF CIVIL DEFENSE’S STATE IN THE REPUBLIC OF SERBIA

Milica Mladenovic^{1a}

¹ S4 Glosec Global security, 15. Maja 13 v, Belgrade, Republic of Serbia,
milica.mladenovic@glosec.rs

Received: 22th August 2023

Accepted: 30th September 2023

Review paper

Abstract: *In years of wars, political tensions, pandemics, energy crises and nuclear threats, the key aspects of civil defense are being re-examined. From the practice of most global community countries, it can be seen that we are entering an era of re-establishment of civil defense, which until now, except in Sweden and Switzerland, whose civil defense systems are at an enviable level, almost did not exist. This paper research the key aspects of the civil defense perception in the Republic of Serbia in the context of contemporary security threats. The perception of civil defense by the relevant subjects represents a complex process of analyzing, interpreting and reviewing the possibilities of prevention and response to all types of crisis situations and enables the research of factors that influence the change in that perception, as well as the ways in which civil defense subjects can communicate with the public in order to improve understanding, trust and cooperation in this areas.*

Key words: *civil defense, Republic of Serbia, perception, state*

1. INTRODUCTION

Security endangerment factors at the global, regional and local level condition the creation of threats to the security of the Republic. All of them lead to destructive activities aimed at the protected values of society, which requires that an effective system of their protection - the civil defense system - be established at the level of the Republic of Serbia. The security threats faced by the Republic of Serbia in recent years require the obligation of all levels of the state organization to create a civil defense system that will be able to respond to them with its institutional and functional organization, and its effectiveness primarily depends on the perception of the importance of the establishment and development of this system. The establishment of a strategically important system, such as the civil defense system, implies the definition of clear postulates on which it will develop and function.

By looking at the existing normative-legal regulations and based on previous research, it is not possible to get a clear picture of the civil defense system of the Republic of Serbia. The problems of the civil defense system have not attracted the interest of many authors, and there is also no progress in the normative regulation of this area. Civil defense is not organized on a

^a ORCID: 0000-0002-8301-0452

systemic approach, it does not have its own organizational and training structure, and the dual responsibilities over the system, which almost does not exist in practice, create additional confusion. The only thing that can be unequivocally concluded is that civil defense represents, in addition to the military, one of the defense pillars of the Republic of Serbia, that, considering the characteristics of modern challenges, risks and threats, its importance is significantly increasing and that it needs to be normatively and legally regulated in as soon as possible in order to obtain an efficient system, capable of reducing the threat of protected values.

The Republic of Serbia civil defense system is a strategic component intended for defense, protection and rescue in peace, war and state of emergency. In recent years, the need for its comprehensive reform within the unified national security system has been recognized, which would ensure the efficient implementation of the function of meeting the needs of the army, state authorities and citizens, and the function of protecting and rescuing the civilian population and material resources. With the growing role and importance of the civil defense system of the Republic of Serbia within the national security system, the need for its faster reform, development and improvement is also growing.

2. PROBLEM DESCRIPTION

The phrase "civil defense" was first mentioned in 1940 in England as the name for the complex protection of the population and elimination of the consequences of bombing (Kastratovic, 2015). In modern theory, there are different definitions and understandings of this term, but they all have in common that it is about the protection of the civilian population and material resources, and that civil structures of society primarily participate in this. As in the world, in our country the phrase "civil defense" is defined in different ways. Jakovljevic, under the system of civil defense means: „an extensive set of non-military measures that ensure the defense, protection and rescue of the population, material and cultural assets and the operation of institutions in situations of drastically impaired functioning of the state system, that is, in war and in conditions of natural disasters and technical-technological an accident in peace” (Jakovljevic, 2006), while Misovic and Kovac define civil defense as „a set of well-organized and functionally coordinated elements, whose actions fulfill the prerequisites for successfully overcoming crisis situations in peacetime and wartime conditions and ensure the best possible conditions for the functioning of all state institutions, especially those that provide services to the entire population” (Misovic & Kovac, 2006). The defense strategy of the Republic of Serbia determines that "civil defense is a part of the defense of the Republic of Serbia focused on preparations for the defense and defense of the Republic of Serbia with non-military means." It is implemented in peace, state of emergency and war through a set of measures and activities aimed at ensuring the successful functioning of state bodies, bodies of autonomous provinces and local self-government units, business companies and other legal entities; creation of conditions for life and work of citizens; meeting the needs of the defense forces; planning and implementation of citizen training plans for the defense of the country; coordination of protection and rescue operations; execution of military, labor and material obligations, as well as mobilization (Strategy of defense of RS, 2019), while in the Law on Defense it is defined as „part of the defense of the Republic of Serbia, which includes a set of measures and activities aimed at: preparations for the defense and defense of the Republic of Serbia with non-military means, ensuring the successful functioning of state bodies, bodies of autonomous provinces and local self-government units, business companies and other legal entities, protection and rescue and provision of conditions for the life and work of citizens and meeting the needs of the defense forces in a state of emergency and war (Law on Defense of the RS, 2018).

Civil defense is an integral part of the country's defense and protection system, which represents a form of civil organization of the state and society with the main goal of protection and defense of protected values. It is an indispensable part of the unified defense system of the Republic of Serbia. Based on the above, it can be concluded that civil defense should represent a set of well-organized and functionally coordinated elements, whose actions fulfill the prerequisites for successfully overcoming various crisis situations in peacetime and wartime conditions. In modern security conditions, the direction of civil defense, its goals and tasks have changed significantly, which must lead to the inclusion of civil defense in the broadest aspects of the protection of all the values of society in all crisis situations.

Civil defense, as a part of the concept of total defense, implies organization on systemic bases and principles that are defined by normative regulations so that the system can fulfill all its functions. The perception of every citizen of the Republic of Serbia, as the most important and most numerous elements of the system, about the place and role in the execution of civil defense tasks at any level of the state organization is a mirror of the possibilities and level of development of the civil defense system and is the starting point for justifying the need and aspiration for its development. As a system that is implemented at all levels of the organization of society, civil defense is faced with numerous problems - from the lack of consensus on the definition of civil defense to inadequate normative-legal regulation and its implementation in practice. It is necessary to redefine civil defense in strategic documents, to organize it as a system with all the necessary elements by normative regulation, to establish a comprehensive system of planning and organization in order to primarily change the perception of all subjects about the importance of civil defense, and then to make the system, which is of strategic importance for the Republic of Serbia, has unequivocally taken its place in the national security system.

3. RESEARCH METHODS DESCRIPTION AND APPLICATION

The research results on the paper topic were obtained by applying all the basic methods of scientific thinking and research. Of the general scientific methods, the hypothetical-deductive method, historical, comparative and statistical method was applied. Data collection for research purposes was carried out using the method of content analysis and the method of examination. The research instrument - a survey - was used for the research. Data on the perception of the elements that are necessary for the existence of the civil defense system and the impact of those elements on the development of the system were collected using the survey method (Mladenovic, 2023).

Due to the specificity of the research subject, for the research participants i.e. experts in the subject area were chosen from the organizational units of the Ministry of Defense and the Serbian Armed Forces, the Ministry of Internal Affairs, state bodies, bodies of autonomous provinces and local self-government units, public companies, business companies and other legal entities, entrepreneurs and civilians, i.e. all subjects of the civil system defense. The opinion was also requested from persons who had professional experience in the field of civil defense. As experts in the subject area were chosen persons whose competences were determined by a combination of the functional and behavioral competence model, which implies that experts in the subject area are not only highly qualified in the field of the subject of research, but also possess the ability to learn quickly, adapt to changes, communicate effectively and improve interpersonal relations (Rodriguez & et al., 2002). The functional model of competencies is associated with the quality of work performance in a specific field of work and the possession of knowledge and skills that enable above-average performance in its performance (Wickramasinghe & Zoyza, 2011). The behavioral competency model refers to the behaviors and abilities of subject area experts such as attitudes, motivations and personal

traits. The survey of experts in the subject area was carried out by filling out a questionnaire with a prior agreement and explanation of the method, goals and significance of the research. The questionnaire contains elements for assessing the competencies of experts in the field (A Global Competency Framework Human Resources Implementation Guide, 2014) based on a combination of functional and behavioral (Boyatzis, (2008)) models for determining competencies (Korn Ferry Leadership Architect Global Competency Framework Legacy Mapping, 2014). Competences of experts are determined in two parts. In the first part, the level of education of the respondent, years of work experience in the field of the research subject, title, position and organization in which the respondent is employed, the sector to which belongs, received awards of the respondent, as well as scientific and professional publications in the field of the research subject. In the second part of the determination of competences, a self-assessment of the competences is carried out for which descriptions (descriptors) are given. The expert in the subject area within the framework of this research possesses competencies according to both models. By combining the functional and behavioral model for determining competencies, were selected subject matter experts who:

- have comprehensive knowledge of the research subject and the ability to use it effectively,
- can perform a wide range of tasks within the subject of research,
- can improve and progress in the field of the research subject,
- possess appropriate personal and professional values and abilities that enable obtaining reliable information.

A statistical method was used to present the research results. In this research, the sample size was determined using the statistical method, the numerical data were analyzed and the obtained results were processed. This method made it possible to systematize the data in order to observe certain regularities and cause-and-effect relationships between the perception of the civil defense system and the level of its development in the Republic of Serbia. The research was carried out on a selected partial statistical sample, composed of part of the subjects of the strategic, operational and tactical level of management in the Republic of Serbia. The statistical unit in the sample consists of individuals - experts in the subject area from the organizational units of the Ministry of Defense and the Serbian Army, the Ministry of Internal Affairs, state bodies, public administration bodies, bodies of autonomous provinces and local self-government units, companies and other legal entities, as well as citizens.

A representative sample was determined based on the formula for calculating the sample size in cases when it is unknown or too large (Field, 2009), (the civil defense system includes all human and material resources of the Republic of Serbia):

$$n = \frac{z^2 \cdot p \cdot q}{e^2} \quad (1)$$

where in:

n – sample size

z - normalized deviation, determined based on the selected confidence level, which in this research is 95%, so the value of z = 1.96.

p – variation for the sample i.e. the probability that respondents will choose a particular answer. Given that 5 answers were offered in the survey, the variation amounts to 20%, i.e. p = 0.2

q = 1-p which means q is 0.8

e – represents the permissible error. The permissible error in the research is 10%, so e=0.1

$$n = \frac{1,96^2 \cdot 0,2 \cdot 0,8}{0,1^2}$$

$$n = \frac{0,614656}{0,01}$$

$$n = 61,4656$$

The size of the representative sample according to the given formula is 61. A total of 73 questionnaires were sent, and 67 responses were received.

4. RESEARCH RESULTS

The conducted research resulted in the perception of the Republic of Serbia's civil defense by relevant subjects at all levels of the state organization, as well as the necessary elements for its development and re-establishment (Mladenovic, 2023).

In accordance with the assessed challenges, risks and threats, the Republic of Serbia should establish an efficient and effective system of civil defense, because civil defense is an activity of strategic importance for the Republic of Serbia in the opinion of experts in the subject area (Figure 1).

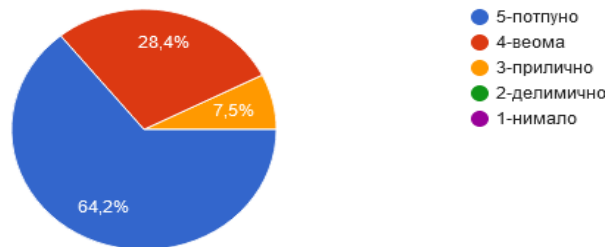


Figure 1. Civil defense is an activity of strategic importance for the Republic of Serbia
Source: Mladenovic, 2023

The opinion of most respondents is that the establishment and improvement of the civil defense system begins with determining its place and role within the defense system, which is currently not the case in practice (Figure 2).

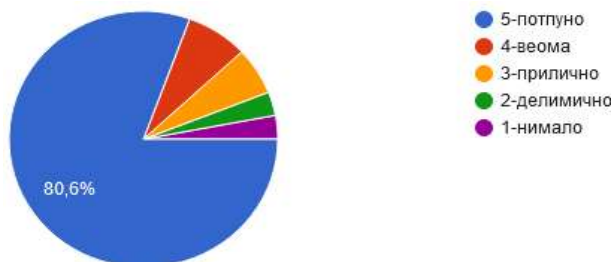


Figure 2. It is necessary for the civil defense system to exist within the defense system of the Republic of Serbia
Source: Mladenovic, 2023

The results of the research showed that the opinion of most respondents is that the Republic of Serbia does not currently have a fully developed civil defense system in practice (Figure 3).

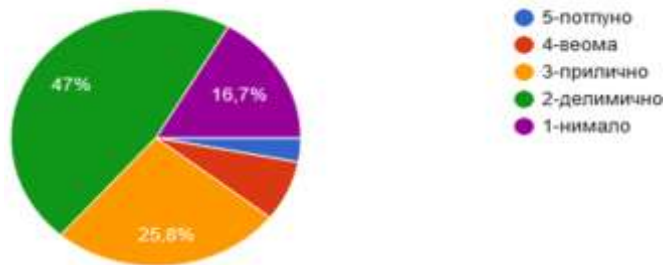


Figure 3. In practice, the Republic of Serbia has an efficient and effective civil defense system

Source: Mladenovic, 2023

Based on the results of the research, it can be concluded that it is necessary, in a systematized way, to establish a comprehensive normative-legal framework of the civil defense system of the Republic of Serbia as a primary step in its construction and development (Figure 4). 65.2% of respondents fully agree with this statement.

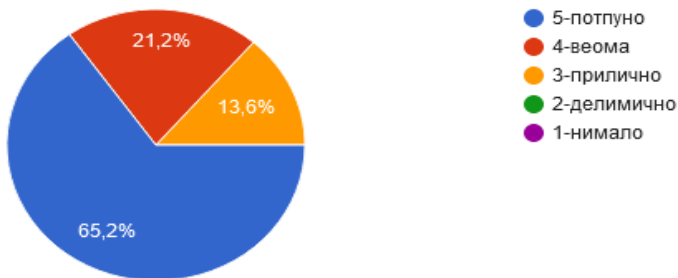


Figure 4. It is necessary, in a systematized way, to establish a comprehensive normative-legal framework of the civil defense system of the Republic of Serbia

Source: Mladenovic, 2023

The organization of the civil defense system should follow the territorial structure of the Republic of Serbia, i.e. it should be developed according to the administrative-territorial division of the state and be represented at all levels of the state organization according to the opinion of 62.1% of experts in the subject area. 22.7% of respondents strongly agree with this statement, while four quite agree, four partially agree, while two do not agree at all (Figure 5).

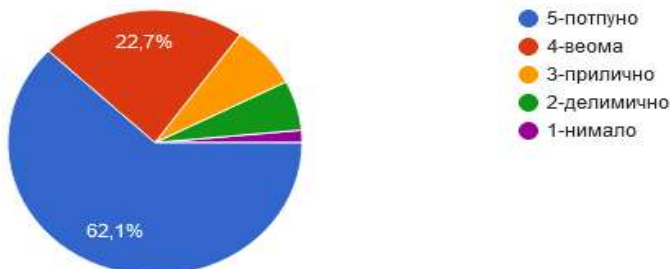


Figure 5. The civil defense system should be organized according to the territorial organization of the Republic of Serbia

Source: Mladenovic, 2023

The establishment of the governing body of the civil defense system should also be carried out at all other levels of the state organization, in which 60% of experts in the subject area completely agree (Figure 6).

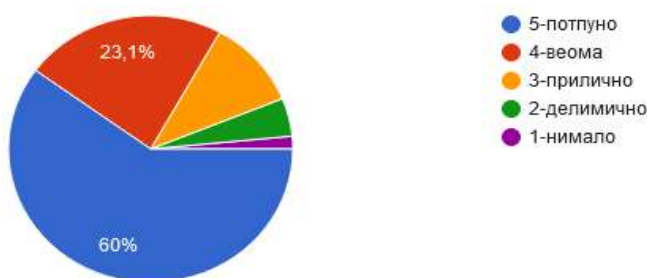


Figure 6. It is necessary to establish a body for managing the civil defense system at all levels of the state organization

Source: Mladenovic, 2023

A prerequisite for the active participation of all subjects in the civil defense system is an appropriate education system (Figure 7). That it is necessary to establish an education system for the needs of the functioning of the civil defense system at all levels of education, 69.7% of experts in the subject area completely agree, 21.2% of them agree at a high level, three partially agree, while one respondent partially agrees, but there is no area expert who expressed disagreement with the given statement.

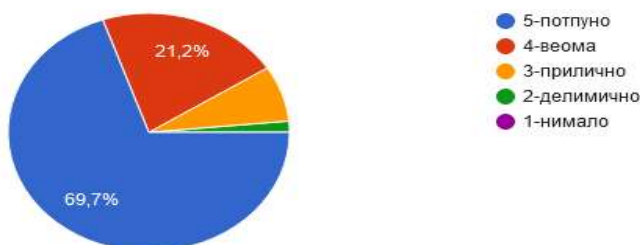


Figure 7. It is necessary to establish an education system for the needs of the functioning of the civil defense system at all levels of education

Source: Mladenovic, 2023

The civil defense system, in accordance with its goals and tasks, is a very complex system that requires comprehensive preparation and permanent development of all its elements. Since there is no detailed structure and adequate organization of the system in the normative regulations of the Republic of Serbia, this research has created certain conditions for its construction and improvement.

5. CONCLUSION

The perception of the civil defense's state in the Republic of Serbia indicates the need for the establishment of a system, its further improvement and harmonization with the modern security situation. The current situation shows the need to take the initiative and invest in forming a system, training and equipping human resources, modernizing equipment and establishing effective preparations for responding to all crisis situations, because the (non)existing system indicates the need for better coordination between different levels of management, as well as for greater involvement of citizens in preventive activities. In this context, it is important to continue strengthening all system capacities. All steps towards

achieving a comprehensive and efficient system cannot be taken at once, but priorities must first be determined that will enable further development and progress. To initiate the establishment of the system, the purpose of the existence of civil defense must first be defined, then it is necessary to determine the state of existing and required human and material resources, and after that to precisely define the normative framework and ensure coordination with all relevant entities, in order to carry out implementation of the system in practice. Given that it represents a system of general social importance, its functioning, establishment and development must be primarily scientifically based. This, in addition to everything, requires the creation of a completely new perception of the system, raising of the level of security culture for everyone in this area, and the formation of a completely new profession that will enable the efficient development of the system.

Based on the presented research on the perception of civil defense state in the Republic of Serbia, it can be concluded that the establishment and development of this system reflects a vital role in ensuring an effective response to potential crisis situations, while at the same time strengthening society's ability to protect its citizens and resources in accordance with modern standards and best practice.

REFERENCES

A Global Competency Framework Human Resources Implementation Guide (2014), Workitect, Florida, USA.

Boyatzis, R.E., (2008): Competencies in the 21st century, Journal of Management.

Defense Strategy of the Republic of Serbia, Official Gazette of the RS No. 94/2019.

Field, A. (2009): Discovering Statistics Using SPSS, 3rd Edition, Sage Publications Ltd., London.

Jakovljevic, V. (2006): Civil Defense, Faculty of Civil Defense, Belgrade.

Kastratovic, L. (2015): Development of the Civil Defense System in the Republic of Serbia - New Model, Faculty of Security, Belgrade,.

Korn Ferry (2014): Leadership Architect Global Competency Framework Legacy Mapping.

Law on Defense, Official Gazette of RS no. 116/2007, 88/2009, 104/2009, 10/2015 and 36/2018.

Misovic, S., Kovac, M. (2006): Defense system, Faculty of Security, Belgrade.

Mladenovic, M. (2023): Development of the civil defense of the Republic of Serbia in the function of reducing the vulnerability of the civilian population and material resources, doctoral dissertation, Military Academy, Belgrade.

Rodriguez, D., Patel, R., Bright, A., Gregory, D. & Gowing, M.K. (2002): Developing Competency Models to Promote Integrated Human Resource Practices', Human Resource Management, 41(3), 309–324, Wiley Periodicals, Inc.

Wickramasinghe, V., Zoyza D. N. (2011): Managerial competency requirements that enhance organizational competencies: a study of a Sri Lankan telecom organization', The International Journal of Human Resource Management, 22(14).

THE DIBR-SAW MODEL FOR THE SELECTION OF LOCATION FOR OVERCOMING WATER BARRIER WITH DEEP DRAFT

Katarina Dojic¹, Darko Bozanic^{2a}, Jovica Milicevic³

¹ University of Defence in Belgrade, Military Academy, Veljka Lukic Kurjaka 33, Belgrade, Republic of Serbia, kacadojic@gmail.com

² University of Defence in Belgrade, Military Academy, Veljka Lukic Kurjaka 33, Belgrade, Republic of Serbia, dbozanic@yahoo.com

³ University of Defence in Belgrade, Military Academy, Veljka Lukic Kurjaka 33, Belgrade, Republic of Serbia, jovicamilicevic74@gmail.com

Received: 28th August 2023

Accepted: 4th September 2023

Original scientific paper

Abstract: *In this paper the issue of selecting a location for overcoming water barrier with deep draft using hybrid model based on the Defining Interrelationships Between Ranked criteria (DIBR) method and the Simple Additive Weighting (SAW) method is discussed. The DIBR method is used to define the weight coefficients of criteria, while the SAW method is used to rank the alternatives. The criteria conditioning the overcoming of water barrier with deep draft are elaborated through the paper. Five experts from the field of overcoming water barriers participated in the research.*

Key words: *location, multi-criteria decision-making, DIBR, SAW*

1. INTRODUCTION

Decision-making is very significant segment of an individual's life (Adegbola, 2023; Debnath & Ghosh, 2021), as well as of various organizational systems (Pamucar et al., 2012; Badi et al., 2023). The importance of making the best decision can be clearly observed through the increased number of research related to the topic of decision-making (Tripathy, 2023). In contemporary scientific literature, there has been a significant increase in the number of methods dealing with multi-criteria decision-making (Si & Ganguly, 2021).

Crossing rivers, as well as water barriers in general, is very complex tactical action, especially when the defended barrier is reinforced with artificial, primarily mine-explosive and fortification obstacles (Bozanic, 2017). Therefore, the Army pays special attention to the decision-making process (Pamucar et al., 2011a). During combat operations, unit commanders find themselves in the situations in which they have to make a large number of more or less significant decisions (Pamucar et al., 2016). The main goal is to make the best decision in the shortest period of time, because making the wrong decision can have catastrophic

^a ORCID: 0000-0002-9657-0889

consequences that are reflected in the loss of personnel and material resources (Pamucar & Bozanic, 2010). In this context, the application of multi-criteria decision-making methods presents an essential support to the mentioned process (Boskovic et al., 2023). For the purposes of this paper, a mathematical model is developed that supports making the decision on the selection of a location for overcoming water barrier with deep draft.

A place of overcoming water barrier with deep draft is intended for tank crossing with a maximum depth of 2.1 meters (Pifat, 1980), and it has a number of specifics that need to be ensured in order to successfully overcome water barrier. The location is selected based on several criteria, using the DIBR and the SAW methods. The essence of the problem lies in the selection of one variant of the decision, which is chosen based on the comparison of all elaborated options (alternatives). In certain situations, there is a possibility that a commander will not have enough knowledge and experience, which can result in making a wrong or lower-quality decision (Pamucar et al. 2011b). By applying a multi-criteria decision-making model, this problem is greatly reduced.

2. DESCRIPTION OF THE DECISION-MAKING MODEL

This paper presents a decision-making supporting model for selecting a location for overcoming water barrier with deep draft using the DIBR and SAW methods.

In the first phase of the model, the criteria are identified and the weight coefficients of the criteria are defined. Hence, certain criteria are defined that influence the solution of the given problem. Using the DIBR method, the weight coefficients of the defined criteria are calculated. In the second phase, the alternatives are defined and the best one is selected using the SAW method. The description of the applied methods is provided below.

2.1. DIBR method

The DIBR method was first presented in the paper by Pamucar et al. (2021). In the following part will be presented the procedure for implementing the DIBR method through 5 steps (Pamucar et al., 2021):

Step 1: Ranking the criteria according to their significance

If there is a defined set of n criteria $C = \{C_1, C_2, C_3, \dots, C_n\}$, it is necessary to rank those criteria according to significance - from the most significant to the least significant criterion. For the purpose of easier presentation of the methodology, the criteria can be ordered according to significance as $C_1 > C_2 > C_3 > \dots > C_n$, where n presents the total number of criteria in the set C .

Step 2: Comparison of criteria and definition of mutual relations

The values that a decision maker assigns to the criteria during the comparison are marked with δ_{ij} , respectively, when comparing the criterion C_1 with the criterion C_2 , the value δ_{12} is assigned, when comparing the criterion C_2 with the criterion C_3 , the value δ_{23} is assigned, and so on until the last criterion.

All the values obtained $\delta_{12}, \delta_{23}, \dots, \delta_{n-1,n}$ и $\delta_{1,n}$ should meet the condition where $\delta_{n-1,n}, \delta_n \in [0, 1]$. Based on this, the following relations between the criteria can be defined:

$$\varphi_1 : \varphi_2 = (1 - \delta_{12}) : \delta_{12} \tag{1}$$

$$\varphi_2 : \varphi_3 = (1 - \delta_{23}) : \delta_{23} \tag{2}$$

...

$$\varphi_{n-1} : \varphi_n = (1 - \delta_{n-1,n}) : \delta_{n-1,n} \tag{3}$$

$$\varphi_1 : \varphi_n = (1 - \delta_{1,n}) : \delta_{1,n} \quad (4)$$

The equations (1) - (4) and the value $\delta_{n-1,n}$ can be observed as the ratios by which the decision maker divides the total interval, whose value is 100%, on the two observed criteria. For example, if the assigned value for $\delta_{12} = 0,45$ this means that the criterion C_1 has 55% of significance, and the criterion C_2 has 45% significance.

Step 3: Defining relations for the calculation of weight coefficients

After the comparison of the criteria and the definition of mutual relations have been performed, the expressions can be derived for defining the weight coefficients of the criteria $\varphi_2, \varphi_3, \dots, \varphi_n$. From the equations (1) - (3), follows next:

$$\varphi_2 = \frac{\delta_{12}}{(1 - \delta_{12})} \varphi_1 \quad (5)$$

$$\varphi_3 = \frac{\delta_{23}}{(1 - \delta_{23})} \varphi_2 = \frac{\delta_{12} \delta_{23}}{(1 - \delta_{12})(1 - \delta_{23})} \varphi_1 \quad (6)$$

...

$$\varphi_n = \frac{\delta_{n-1,n}}{(1 - \delta_{n-1,n})} \varphi_{n-1,n} = \frac{\delta_{12} \cdot \delta_{23} \cdot \dots \cdot \delta_{n-1,n}}{(1 - \delta_{12})(1 - \delta_{23}) \cdot \dots \cdot (1 - \delta_{n-1,n})} \varphi_1 = \frac{\prod_{i=1}^{n-1} \delta_{i,i+1}}{\prod_{i=1}^{n-1} (1 - \delta_{i,i+1})} \varphi_1 \quad (7)$$

Step 4: Calculation of the weight coefficient of the most influential criterion

On the basis of the equations (5) - (7) and having been met the condition where $\sum_{j=1}^n \varphi_j = 1$, it is possible to obtain the expression for the calculation of the weight coefficient of the most influential criterion:

$$\varphi_1 = \frac{1}{1 + \frac{\delta_{12}}{(1 - \delta_{12})} + \frac{\delta_{12} \delta_{23}}{(1 - \delta_{12})(1 - \delta_{23})} + \dots + \frac{\prod_{i=1}^{n-1} \delta_{i,i+1}}{\prod_{i=1}^{n-1} (1 - \delta_{i,i+1})}} \quad (8)$$

By applying the already defined equations (5) - (7), the values of the other weight coefficients are determined $\varphi_2, \varphi_3, \dots, \varphi_n$.

Step 5: Calculation of the aggregated weight coefficients of criteria

Through the first four steps, the weight coefficients of criteria are calculated for each expert separately. In this step, the experts' opinions are aggregated into one value. The aggregation is performed using the Bonferroni Mean operator:

$$BM^{p,q}(\Phi_1, \Phi_2, \dots, \Phi_n) = \left[\frac{1}{n(n-1)} \sum_{\substack{i,j=1 \\ i \neq j}}^n \varphi_i^p K \varphi_j^q \right]^{\frac{1}{p+q}} \quad (9)$$

where $p, q \geq 0$ presents stabilization parameters of the Bonferroni operator.

2.2. SAW method

The SAW method was developed by Churchman and Ackoff (1954). Although it is an older method, the results obtained with it are very similar to the results of a large part of modern methods. The same as with other methods, the initial decision-making matrix is defined at the beginning.

$$M = \begin{matrix} & C_1 & C_2 & C_3 & \dots & C_n \\ \begin{matrix} A_1 \\ A_2 \\ A_3 \\ \vdots \\ A_m \end{matrix} & \begin{bmatrix} x_{11} & x_{12} & x_{13} & \dots & x_{1n} \\ x_{21} & x_{22} & x_{23} & \dots & x_{2n} \\ x_{31} & x_{32} & x_{33} & \dots & x_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{m1} & x_{m2} & x_{m3} & \dots & x_{mn} \end{bmatrix} \end{matrix} \quad (10)$$

The SAW method is very simple and involves only three steps, which are presented below.

Step 1: Normalization of the initial decision-making matrix

The authors of the method did not define the type of normalization to be used. Linear normalization is used in this paper:

$$n_{ij} = \frac{x_i^{\min} - x_{ij}}{x_i^{\min} - x_i^{\max}} \quad (11)$$

$$n_{ij} = \frac{x_i^{\max} - x_{ij}}{x_i^{\max} - x_i^{\min}} \quad (12)$$

where x_{ij} presents the specific value of a criterion for certain alternative, x_i^{\max} is the highest value of a criterion among the offered alternatives and x_i^{\min} is the lowest value of a criterion among the offered alternatives. The expression (11) is applied to define benefit-type criteria. On the other hand, the expression (12) is used to define cost-type criteria.

Step 2: Weighting of normalized matrix

Weighting of normalized matrix is made according to the expression (13).

$$D = \begin{bmatrix} v_{11} & \dots & v_{1j} & \dots & v_{1n} \\ \vdots & & \vdots & & \vdots \\ v_{i1} & & v_{ij} & & v_{in} \\ \vdots & & \vdots & & \vdots \\ v_{m1} & \dots & v_{mj} & \dots & v_{mn} \end{bmatrix} = \begin{bmatrix} \Phi_1 n_{11} & \dots & \Phi_j n_{ij} & \dots & \Phi_n n_{1n} \\ \vdots & & \vdots & & \vdots \\ \Phi_1 n_{i1} & & \Phi_j n_{ij} & & \Phi_n n_{in} \\ \vdots & & \vdots & & \vdots \\ \Phi_1 n_{m1} & \dots & \Phi_j n_{mj} & \dots & \Phi_n n_{mn} \end{bmatrix} \quad (13)$$

Step 3: Summing the weighted ratings for each alternative

In this step, the weighted values for each alternative are summed up.

$$S_j = \sum_{j=1}^m \varphi_j x_{ij}, \quad (14)$$

$j = 1, 2, \dots, m,$

This sum provides each alternative with certain utility. When making a decision, it should be selected the alternative with the greatest utility.

3. APPLICATION OF THE DECISION-MAKING MODEL

In order to start solving the issue with multi-criteria decision-making model, first it is necessary to define and rank the criteria in the manner described in the first step of the DIBR method. For the purposes of this paper, five experts are surveyed, who defined the criteria, ranked and compared them. According to the views of the experts, the following eight criteria are defined:

– *Depth of water barrier (C1)* - distance measured from the surface to the bottom of water barrier;

– *Speed of water barrier (C2)* - speed of water movement per unit of time [m/s];

- *Width of water barrier (C3)* - distance between the banks, measured by the surface of water obstacle;
- *Scope of works on the arrangement of the bottom (C4)* - largely depends on the geological composition of the bottom;
- *Scope of works on the arrangement of enemy bank (C5)* - works such as the arrangement of bank height, bank slope, removal of various natural and artificial obstacles on the bank, etc.;
- *Scope of works on the arrangement of own bank (C6)* - includes similar works as in the arrangement of the enemy's bank;
- *Conditions for masking (C7)* - the forested area should be used to the maximum for masking when preparing to overcome water barriers;
- *Access roads (C8)* - the roads allowing the access of units to and from water barrier.

The first three criteria are numerical ones, while the other criteria are of linguistic character, described by a five-point scale (1,3,5,7,9).

Based on the opinion of the experts, all the mentioned criteria are defined according to significance. The weights of criteria (φ) are obtained by applying the expressions (1) - (8). After the calculation, the weight coefficients of the criteria are aggregated using the Bonferroni Mean operator (the expression 9). The final results of the weight coefficients of the criteria are presented in the Table 1.

Table 1. Weight coefficients of the criteria (Source: Authors)

Criteria	Φ_i
C1	0,408
C2	0,136
C3	0,223
C4	0,071
C5	0,044
C6	0,031
C7	0,021
C8	0,028

Once the weight coefficients of the criteria are calculated, the selection of the best alternative is made. At the beginning, a decision-making matrix is created to which the SAW method is directly applied. The Table 2 shows the quantified values for 10 virtual alternatives for each criterion.

Table 2. Quantified initial decision-making matrix (Source: Authors)

Alternatives	C1	C2	C3	C4	C5	C6	C7	C8
A1	2,01	0,55	351	5	1	3	4	3
A2	1,53	1,25	416	9	9	1	2	1
A3	1,68	1,61	521	3	5	9	1	5
A4	1,02	1,76	603	1	7	5	3	2
A5	1,96	1,07	498	5	3	7	5	4
A6	2,06	0,94	385	1	3	5	1	2
A7	1,48	0,56	569	7	9	9	3	3

Alternatives	C1	C2	C3	C4	C5	C6	C7	C8
A8	1,71	1,43	618	7	5	3	4	5
A9	2,05	0,38	447	3	1	1	5	1
A10	1,88	0,24	652	9	7	7	2	4
Type of Criteria	cost	cost	cost	cost	cost	cost	benefit	benefit

By practical application of the further steps of the SAW method, the calculation is performed. Each alternative received certain utility determining its position in the ranking list. The ranking list of alternatives is given in the Table 3.

Table 3. Ranking of alternatives (Source: Authors)

Alternatives	Q _j	Ранг
A1	0,484	2
A2	0,465	3
A3	0,363	7
A4	0,560	1
A5	0,333	8
A6	0,398	6
A7	0,438	4
A8	0,299	9
A9	0,429	5
A10	0,251	10

The results from the Table 3 show that in this particular example, the best alternative for overcoming water barrier with deep draft is the alternative A4. The alternatives A1 and A2 are in the second and third place. These could be chosen as favorable solutions in certain situations. In the last place is the alternative A10.

4. CONCLUSION

This procedure provided the conditions for quick quality decision-making in the process of selecting a location for tanks crossing water barriers with deep draft. Undoubtedly, decision-making becomes one of the key elements in creating business environment in the upcoming period, especially in the situations where human lives and material goods are at risk. Apart from the practical contribution of the paper, from the theoretical aspect, the conceptualization of a relatively new method for defining weight coefficients of criteria - DIBR, as well as its successful application in practice, is presented. The output results obtained using the SAW method show that the method can be used as a decision-making support. The greatest contribution provided by the applied model is reflected in the fact that potential errors in a decision-making process are reduced to a minimum by the use of mathematical solutions.

REFERENCES

- Adegbola, K. (2023). A simulation study of single-vendor, single and multiple-manufacturers supply chain system, with stochastic demand and two distribution policies, *Journal of Decision Analytics and Intelligent Computing*, Vol. 3 (No. 1).
- Badi, I., Stevic, Z., Bayane Bouraima, M. (2023). Overcoming Obstacles to Renewable Energy Development in Libya: An MCDM Approach towards Effective Strategy Formulation. *Decision Making Advances*, Vol. 1 (No. 1).

- Boskovic, S., Svadlenka, L., Dobrodolac, M., et al (2023). An Extended AROMAN Method for Cargo Bike Delivery Concept Selection. *Decision Making Advances*, Vol. 1 (No. 1).
- Bozanic, D. (2017). Model of decision support in overcoming water obstacles in Army combat operations, (Only in Serbian: Model podrške odlucivanju pri savladivanju vodenih prepreka u napadnoj operaciji Kopnene vojske), doctoral dissertation, University of Defence in Belgrade, Military Academy, Belgrade.
- Bozanic, D., Pamucar, D. (2010). Evaluating locations for river crossing using fuzzy logic, *Military Technical Courier*, Vol. 58 (No. 1).
- Churchman, C.W., Ackoff, R.L. (1954). An approximate measure of value, *Journal of Operations Research Society of America*, Vol. 2 (No. 1).
- Debnath, S., Ghosh, S. (2021). Experimental investigation of Electro discharge machining process by AHP-MOORA technique. *Journal of Industrial Engineering and Decision Making*, Vol. 2 (No. 1).
- Pamucar D., Bozanic D., Djorovic B, et al. (2011a). Modelling of the fuzzy logical system for offering support in making decisions within the engineering units of the Serbian army, *International Journal of the Physical Sciences*, Vol. 6 (No. 3).
- Pamucar, D. Bozanic, D., Djorovic, B. (2011b). Fuzzy logic in decision making process in the Armed Forces of Serbia, LAP Lambert Academic Publishing & Co. KG, ISBN: 978-3-8443-8805-3, Saarbrücken.
- Pamucar, D., Bozanic, D., Milic, A. (2016). Selection of a course of action by obstacle employment group based on a fuzzy logic system, *Yugoslav Journal of Operations Research*, Vol. 26 (No. 1).
- Pamucar, D., Deveci, M., Gokasar, I., et al. (2021). Circular economy concepts in urban mobility alternatives using integrated DIBR method and fuzzy Dombi CoCoSo model, *Journal of Cleaner Production*, Vol. 323.
- Pamucar, D., Djorovic, B., Bozanic, D., et al. (2012). Modification of the dynamic scale of marks in analytic hierarchy process (AHP) and analytic network approach (ANP) through application of fuzzy approach, *Scientific Research and Essays*, Vol. 7 (No. 1), pp. 24-37.
- Pifat, V. (1980). Savladjivanje vodenih prepreka, Vojnoizdavacki zavod, Beograd.
- Si, A., Ganguly, U. (2021). Drainage and management of offseason rain water in multipurpose reservoir using fuzzy model. *Journal of Industrial Engineering and Decision Making*, Vol. 2 (No. 1).
- Tripathy, S.B. (2023). Bi-objective covering salesman problem with uncertainty, *Journal of Decision Analytics and Intelligent Computing*, Vol. 3 (No. 1).

HYDROTECHNICAL AND HYDROLOGICAL CONDITIONS FOR NAVIGATION IN THE CHANNELS OF THE DANUBE-TISA-DANUBE HYDROSYSTEM

Milorad Tesanovic¹, Vladimir Matijevic², Svetislav Soskic^{3a}

¹ River Flotilla, 1300 kaplara 11, Novi Sad, Republic of Serbia,
tesanovicmilorad@gmail.com

² River Flotilla, 1300 Kaplara 11, Novi Sad, Republic of Serbia, vladematijevic@yahoo.com

³ University of Defense in Belgrade, Military Academy, Veljka Lukica-Kurjaka Street
Belgrade, Republic of Serbia, cacaksole@yahoo.com

Received: 28th August 2023

Accepted: 11th September 2023

Professional paper

Abstract: *the Danube-Tisa-Danube Hydrosystem (Hs DTD) canals and experiences gained during navigation and research will be described. channels Hs DTD in the period from 2010 to 2021 with ships of the River Flotilla . And all in order to verify the accuracy of the data of JVP "VOĐE VOJVODINA" related to the hydrological characteristics of waterways and hydrotechnical characteristics of buildings on Hs DTD.*

Before these voyages, there was no information and data about the voyages of the ships of the River Flotilla in the Hs DTD channels. A survey was conducted before each voyage of the Hs DTD canal and hydrotechnical structures on the canals from the land with the use of motor vehicles and boats in order to measure the height of the free passage on the bridges and measure the depth of the canal due to the draft of the ship. The obtained data can be used for commercial purposes, and as is known, there are no „pilots“ on the Hs DTD channels that can safely guide the ships to the desired location..

Key words: *Danube-Tisa-Danube hydrosystem (Hs DTD), navigation, height of free passage on bridges, depth, ship's draft*

1. INTRODUCTION

The Danube-Tisa-Danube hydrosystem is a unique canal network that connects the flows of the Danube and Tisa rivers through Vojvodina and represents a hydrotechnical system for drainage of internal waters, irrigation , flood defense, water supply, removal of used water, navigation, tourism , fishing and forestry. The DTD hydrosystem with natural and partially reconstructed watercourses has 960 km, of which 600.6 km is navigable: 355.5 km in Backa, and 245.1 km in Banat.

^a ORCID: 0000-0002-6042-8020

Its network connects 80 settlements in Vojvodina, and within the system there are 23 bridges, five security bridges, 15 ship locks and five more that are no longer in operation, five large pumping stations and 86 bridges (64 road, 21 railway and one pedestrian).

At Hs DTD, cargo ships with a carrying capacity of up to 1,000 t can currently sail at 345.3 km, vessels with a carrying capacity of 500 t at 558.3 km and vessels with a carrying capacity of 200 t can sail at 600.6 km. On the Hs DTD channels there are about 30 transshipment places - wharves, specialized wharves and wharves with landfill. The possible annual traffic on Hs DTD waterways is about 7,000,000 t. In the past few years, the turnover is about 1,000,000 t, and the highest achieved turnover was in 1979 and was 4,213,000 t. Types of goods: gravel and sand - 80%, stone - 5%, agricultural products 1 - 2%, wood 3 - 5%, coal, metals, oil and oil derivatives - up to 10%.

2. HYDROTECHNICAL AND HYDROLOGICAL CONDITIONS FOR NAVIGATION ON THE CHANNELS OF THE DANUBE-TISA-DANUBE HYDROSYSTEM

1) Current situation on the Canals of the "Danube-Tisa-Danube" Hydrosystem

The canals of the "Danube-Tisa-Danube" Hydrosystem are of immeasurable importance for the sustainable development of this part of Serbia in terms of regulating the water regime. At the same time, in all phases of its construction, this canal network was designed as a unique waterway integrated into the waterways of the Danube and Tisa rivers in the area of Vojvodina. The total length of the navigable canal network is about 600 km, of which, according to the categorization of state waterways carried out in 2013, 13.1 km is in the Va category, and 289.8 km in the III category. Of the 17 ship locks built in total, 12 are 85 x 12 x 3 in dimensions (including the Brana na Tisza lock) and all are in operation. On the canals of the "Danube-Tisa-Danube" Hydrosystem, the revitalization of endangered sections polluted by silt (Vrbas, Zrenjanin) is needed, as well as the rehabilitation of the Bezdán lock, as the entry point from the Danube to the canal system near the town of Bezdán, which has not been in operation for more than 30 years. .

The authority for technical maintenance of the waterway on the HS DTD canals is JVP "Vode Vojvodina", which is also the manager of this water management facility.



Figure 1. Hydrosystem Danube-Tisa-Danube

Source: [http:// www.vodevojvodine /](http://www.vodevojvodine/)

Characteristics of the channel of the "Danube-Tisa-Danube" Hydrosystem

The total length of the navigable canals of the "Danube-Tisa-Danube" hydrosystem with the course of the Tamis is 664.1 km, which is 47% of the total length of the waterways of Vojvodina, or 41% of the total length of the waterways of Serbia. On them, it is possible to navigate 1,000-ton vessels on 376.9 km, five-hundred-ton vessels on another 258.8 km, and two-ton vessels on the remaining 28.4 km of the canal waterway.

Naziv kanala	Dužina kanala	Deonica (km)		B (m)	B _{vo} (m)		T (m)	Klasa kanala
		od	do		min	max		
Bečež-Bogojevo	90,2	0,0	39,0	27,0	33	200	1,95	III
		39,0	47,5	14,4	37	41	1,95	III
		47,5	90,2	21,5	40	50	1,95	III
Novi Sad-Savino Selo	39,1	0,0	4,4	35,0	46	130	3,00	Va
		4,4	39,1	27,7 ¹⁾	48	54	1,95	III
Vrbas-Bezdan	80,9	0,0	6,3	25,0	36		1,95 ⁴⁾	- ⁵⁾
		6,3	80,9	15,2	22	150	1,80	II
Odžaci-Sombor	27,8	0,0	27,8	21,0	33	40	1,95	III
Bački Petrovac-Karavukovo	52,0	0,0	20,0	18,0	35	37	1,95	I ³⁾
		20,0	40,0	9,6	25	32	1,80	I ³⁾
		40,0	52,0	7,8	25	27	1,15	I
Prigrevica-Bezdan	31,7 ⁴⁾	0,0	31,7	18,0	40	52	1,80	II
Kosančić-Mali Stapar	21,1 ⁴⁾	0,0	3,5	13,5	38		1,95	II
		4,5	21,1	11,5	20		1,30	I
Bezdan-Baja	12,7	0,0	12,7	7,0	20	30	1,30	I
Banatska Palanka-Novi Bečež	147,3	0,0	8,7	54,0	90	160	3,00	Va
		8,7	26,0	44,0	90	100	1,95	III
		26,0	27,5	12,0	35	40	1,95	II
		27,5	45,0	44,0	60	80	1,95	III
		45,0	57,0	33,0	50	60	1,95	III
		57,0	85,0	21,0	40	60	1,95	III
Begej	34,6	0,0	9,2	32,0	33	176	3,00	III
		9,2	34,6	25,0	33	60	1,95	III
Ploveni Begej	31,2	0,0	31,2	17,0	30	40	1,80	II
Kikindski kanal	32,0	0,0	32,0	16,0	35	40	1,80	II

B – širina plovnog puta
B_{vo} – širina vodnog ogledala
T – preporučeni gaz merodavnog plovila

- 1) – na km 23,55 nalaze se ostaci pontonskog mosta čime je sužena širina plovnog puta na 17,2 m
- 2) – na deonici kanala od km 1 do km 6,3 je onemogućena plovidba zbog velikog zamuljenja od otpadnih voda koje se na toj deonici ulivaju u kanal i zbog novo-postavljenog mosta na km 2,6 koji ne omogućuje dovoljnu plovnu visinu od nivoa vode do donje ivice konstrukcije mosta (DJK)
- 3) – kanal je zarastao travom i trskom pri čemu je plovna širina nedovoljna za III odnosno II klasu
- 4) – na km 31,7 nalazi se vodozahvatna ustava Bezdan koja onemogućava plovidbu
- 5) – na km 3,75 i km 4,50 kanal je pregrađen kaskadnim prelivom i ustavom Ruski Krstur koji onemogućavaju plovidbu

Figure 2. Classification of waterways Hs DTD

Source: <https://www.vodevojvodine.rs>

The channel BECEJ - BOGOJEVO (90.0 km) represents the main waterway of Backa. The entrance from the Tisa (km 72.70) is near Becej and goes through the new Becej lock (the old lock has been put out of service), and from the Danube (km 1363.43) through the Bogojevo lock. The translation time depends on the water level of the Tisza and the Danube. The entrances to both locks are perpendicular to the course of the river, which makes it difficult to navigate. In addition to the two external ones, the canal has only one internal lock in Kucura (km 47.3), with a translation duration of about half an hour. The canal connects 15 inhabited places, of which Becej, Srbobran, Vrbas, Backo Gradiste and Ruski Krstur are important as docks and transshipment places.

The forks are at km 8.5 (dead end for Backo Gradiste), km 39.1 (connection with the Vrbas - Bezdan canal), km 53.59 (Fork with the Novi Sad - Savino Selo canal), km 61.86 (fork with

along the Kosancic - Mali Stapar canal), km 78.57 (fork with the Odzaci - Sombor canal) and km 84.05 (fork with the Backi Petrovac - Karavukovo canal).

On this channel, the Odzaci safety pier is located, with two navigable openings of 16 meters each, to ensure two-way navigation. It was built as part of the second defensive line along the line of the average high terrain of the Danube and Tisza watershed. Simultaneous two-way navigation of thousand-ton vessels is possible through the canal, except for the section from km 39.3 to 47.3 (from the fork with the Vrbas-Bezdan canal to the Kucura lock), where only one-way navigation is possible for this category of vessels, or simultaneously two-way for five hundred ton vessels. The channel passes through the bed of Crna Bara (km 9 - km 30), which has a large navigable width. In this section, the ship should be steered carefully due to the large number of dings and large drifts in strong winds.

The NOVI SAD - SAVINO SELO canal (39.11 km) is part of the Small Canal, better known as the Crown Prince Alexander Canal. In terms of importance, the Backa channel is second. It connects the Becej - Bogojevo canal (km 53.59) near Savino Selo with the Danube near Novi Sad (km 1253.4). At km 4.38 is the Novi Sad external lock, which is the only one on the canal. The transfer of the ships lasts from 30 to 40 minutes, depending on the water level of the Danube. Downstream from the Novi Sad lock (km 4.30) a turnpike for ships was built, which is also used as a winter shelter in the winter.

Navigation without translation is possible further from Savino Selo all the way to Bogojevo and Srpski Miletic via the Becej - Bogojevo channel, or Backi Petrovac - Karavukovo, and Odzaci - Sombor channel, then to Kucura and Rusko Krstur via the Becej - Bogojevo and Kosancic - Mali Stapar channels. Along the entire length of the canal, simultaneous two-way navigation of thousand-ton vessels is possible.

The forks of the canal are at km 21.21 (connection with the Backi Petrovac - Karavukovo canal), km 39.10 (connection with the Becej - Bogojevo canal) and km 35.33 (fork with the non-navigable Jegricka canal).

The canal connects seven populated places, the most important of which is Novi Sad, as the largest industrial and agricultural center of Vojvodina.

The VRBAS - BEZDAN canal is known as the Great Canal or the Franz Joseph and King Peter Canal. It is a section of the former Becej-Bezdan canal. Between the fork with the Becej - Bogojevo canal (km 39) as the beginning, and the entrance to the Danube (km 1425.60), as the end, stretches a waterway 80.9 km long.

The forks are located at km 35.40 with the Kosancic–Mali Stapar canal, and km 51.65 with the Odzaci–Sombor canal and km 77.46 with the Bajski canal.

Simultaneous two-way navigation of one-thousand-ton vessels is possible only downstream of the Vrbas lock, while between the Vrbas and Bezdan locks, simultaneous two-way navigation of five-hundred-ton vessels is possible. The Mali Stapar lock is the smallest lock on the network of navigable canals of the "Danube-Tisa-Danube" hydrosystem. Translation at Bezdanska Prevodina takes between 50 and 70 minutes, and 40 minutes each at Mali Stapar and Vrbas.

At km 71.7, a safety bridge Ceská ěuprija was built, with a 12 m wide navigable opening and the basic task of closing the channel to protect it from Danube floodwaters and further flow into Backa.

The canal connects Vrbas, Kula, Crvenka, Backi Monostor and Bezdan.

The ODZACI-SOMBOR canal (27.9 km) connects the Vrbas-Bezdan (km 51.65) and Becej-Bogojevo (km 78.57) canals. It is connected to the Prigrevica-Bezdan canal via a fork at km 21.41. Interpreters are in Srpski Miletic (km 6.06) and Sombor (km 27.4). The canal enables simultaneous two-way navigation of thousand-ton vessels and is a transit route for ships from Novi Sad and Bogojevo that sail to Sombor. There are no docks built on it.

The BACKI PETROVAC - KARAVUKO canal (52.0 km) connects the Becej - Bogojevo canal (km 84.05) near Karavukovo with the Novi Sad - Savino Selo canal (km 21.21) near Backi Petrovac. The Bac safety road at km 33.35 has a width of 16 m and is basically the same as the roads in Kupusina and Odzaci.

The canal enables one-way navigation of thousand-ton vessels on the section from km 0.00 to km 20.0, one-way navigation of five-hundred-ton vessels from km 20.0 to km 40.0, and on the remaining part of the canal, one-way navigation of two-ton vessels.

Canal KOSANCIC – MALI STAPAR (21.1 km). Constitution in Russki Krstur divides this channel into two blind branches. The first leg from Kosancic to Ruski Krstur begins at the fork with the Becej–Bogojevo canal (km 61.86), and ends at the Ruski Krstur junction (km 3.7). One-way navigation of five-hundred-ton structures to the Ruski Krstur pier is possible through this section. There are no turnstiles on it, so vessels must return by sailing astern. The second leg Ruski Krstur–Mali Stapar (16.66 km) allows for one-way navigation of five-hundred-ton vessels and turns in the turnpike near Kruscic. Because of the above, this channel is not of major importance for navigation.

The BAJSKI canal (12.7 km), once Alimentacioni or Sugovicki, is essentially a branch of the Vrbas-Bezdan canal. It starts at the fork of the Vrbas - Bezdan canal at km 77.46. At km 0.16 is the Sebes-fok lock, which has been converted into a safety lock. One-way navigation of five-hundred-ton buildings is possible through the canal. Navigation through this channel has no major economic importance.

The BANAT PALANKA - NOVI BECEJ canal (147.3 km) is the main highway of Banat. The entrance from the Danube (left bank) is at km 1075, and from the Tisa at km 65 through the Novi Becej lock. Two outer locks (Kajtasovo and Novi Becej) and one inner lock (Botos) were built on it. It enables simultaneous two-way navigation for thousand-ton vessels along the entire length, except for the section from km 73.1 to km 87.3, where only one-way navigation is possible for this category of vessels and two-way for other vessels. The forks of the canal are at km 87.8 with Tamis, km 109.1 with Begeja and at km 134.3 with the Kikinda canal. Apart from the forks, turnings are also possible at the mouth of the Brzava (km 75).

BEGEJ Canal (Tisa - Klek) (67 km). The reconstructed Begej canal is from the junction with the Tisza near Titel to Klek (km 34.8). From Tisa to Klek, simultaneous two-way navigation is possible for thousand-ton objects. It is characteristic that this channel has the water level of Tisa up to Stajicevo. When sailing, you should take into account the water level values, which are extremely high in certain periods, which is why passing under bridges can be a problem. The canal connects Perlez and Zrenjanin, which is the industrial and agricultural center of Banat, with the Begej shipyard.

Navigable BEGEJ (Klek - state border) (29 km). From Klek to Itebej, it passes along the old route of Begeja. Simultaneous two-way navigation for five-hundred-ton objects is possible on this channel. The canal connects Itebej, Begejce and Zitiste.

The KIKIND channel begins at the fork with the Banatska Palanka–Novi Becej channel at km 134.3, and ends at the junction with Zlatica. With its length of 50.3 km, it enables one-way navigation for one-thousand-ton objects and simultaneous two-way navigation for five-

hundred-ton objects. There are no locks on the canal. It is connected to the Tisa waterway by the Banatska Palanka–Novi Becej canal, through the lock in Novi Becej, and by the Begej canal through the Stajicevo lock.

The river TAMIS , from the aspect of navigation, has two parts. One part of the stream is channeled, namely on the stretch from Tomasevac to Jasa Tomic, and enables the one-way navigation of one-thousand-ton objects and the simultaneous two-way navigation of five-hundred-ton objects. The second part of the Tamis stream, which is not navigably connected to the first, goes from the confluence with the Danube near Pancevo, in a length of another 3 km, on which part is the Pancevo lock.

3. HYDROTECHNICAL BUILDINGS ON THE DANUBE-TISA-DANUBE HYDROSYSTEM CHANNELS

(1) Dam

The dam on the Tisza near Novi Becej was completed in 1977 and is the largest facility on the DTD Hydrosystem. The dam has seven spillways and a lock for ships up to 1000 tons. With its construction and raising the level of the Tisa upstream, gravity catchment was enabled, that is, the supply of the Banat area with water from the DTD Hydrosystem. The 520 m long Tisa river bed is blocked by a dam for high water. A road bridge was designed on the pillars of the dam, as a traffic connection between Banat and Backa.



Figure 3. Dam on the Tisza
Source: Photographed on a voyage in 2012

(2) Ship Locks

10 new locks were built on the DTD canal, while five old locks were connected to the Hydrosystem. Some old locks today serve as prisons. There is also a lock in the structure of the Tisza dam. The role of the lock is to translate ships from one level of water to another.

Old locks: Backi Monostor (not in operation); Backo Gradiste (not in operation); Vrbas (today Vrbas Constitution); Little Stapar; Serb; Bezdán (reconstructed on September 25, 2020); Becej - old (today a cultural monument); Serbian Itebej; Klek.

New locks: Sombor; Serbian Miletic; Bogojevo; Novi Sad; A bitch; Becej; Vrbas; Novi Becej; Stajic's; Botos; Kajtasovo.

Kanal	km kanala	Naziv prevodnice	Karakteristike komore prevodnice			Br. telefona
			Dužina (m)	Širina (m)	Đubina ¹⁾ (m)	
Bečež - Bogojevo	0,16	Bečež	85,0	12,0	3,0	066/8642-225
	47,30	Kucura	85,0	12,0	3,0	066/8642-226
	89,45	Bogojevo	85,0	12,0	3,0	066/385-643
Novi Sad - Savino Selo	4,30	Novi Sad	85,0	12,0	3,0	066/8642-341
Vrbas - Beždan	6,20	Vrbas ²⁾	85,0	12,0	3,0	063/888-6312
	34,40	Mali Stapar ⁴⁾	62,4	8,1	2,5	
	80,80	Beždan ⁴⁾	68,0	9,1	2,5	
	70,3	Pontonski most				
Odžaci - Sombor	6,00	Srpski Miletić	85,0	12,0	3,0	066/8642-381
	27,40	Sombor	85,0	12,0	3,0	066/8642-383
Bajski kanal	0,16	Šebežfok ³⁾	69,0	9,4	2,5	066/8642-259
Banatska Palanka – Novi Bečež	8,70	Kajtasovo	85,0	12,0	3,0	066/8091-087
	85,60	Botoš	85,0	12,0	3,0	066/8642-181
	147,20	Novi Bečež	85,0	12,0	3,0	066/8643-052
Kanal Begej	9,20	Stajičevo	85,0	12,0	3,0	066/8642-182
Kanal Plovni Begej	0,70	Klek, donja ⁵⁾	64,0	9,7	2,4	
	0,80	Klek, gornja	72,1	9,7	2,4	
	29,0	Srpski Itebej ⁶⁾	72,1	9,7	2,4	
Reka Tisa	63,0	Brana na Tisi	85,0	12,0	3,0	066/8643-051

1) – Dubina vode pri minimalnom vodostaju
2) – Prevodnica Vrbas nije u funkciji
3) – Prevodnica Beždan nije u funkciji čime je prekinuta veza sa Dunavom u pogledu plovidbe
4) – Prevodnica Mali Stapar radi na ručni pogon i u jako je lošem stanju te se ne preporučuje prevođenje
5) – Prevodnica Šebežfok radi kao ustava i omogućuje prolaz manjih plovila (jahti i čamaca) koji su na ekološki pogon, samo pri određenim hidrološkim i vodnoredžimskim uslovima
6) – Prevodnice Klek i Srpski Itebej nisu u funkciji

Figure 4. Characteristics of locks on Hs DTD channels

Source: <https://www.vodevojvodine.rs>

(3) Constitution

On the basic canal network of the Hidrosystem DTD, there are 23 constitutions, 18 new ones and five constitutions that existed even before Nikola Mirkov started building the Hidrosystem. Constitutions were built as independent facilities or together with locks as part of the hydro node. The task of the constitution is to regulate the water level in the canal. Constitutions bear the names of the places where (or next to) they were erected, and are located in the following places:

- | | |
|-------------------|-------------------------------------|
| – Abyss | – Fall down |
| – Serbian Miletic | – Sajan - (constitution in Zlatica) |
| – Novi Sad | – Itebej and Klek |
| – A bitch | – Stajic's |
| – Russian Krstur | – Botos |
| – Vrbas | – Tomasevac |
| – Despot's | – Centa |
| – Dragon | – Again |
| – Frog | – Pancevo |
| – Little Stapar | – Kajtasovo |
| – Novi Bečež | |

(4) Security constitutions

Safety structures are located on the channels of the Hidrosystem in Backa. There are five of them and they form a system that prevents the intrusion of flood waters from the Danube into the central and southern parts of Backa. They are constructed in such a way that navigation is possible through them, and they can also let in adequate amounts of water for irrigation. The security constitutions are:

- Shebeshfok
- Czech bridge
- Cabbage
- Chimneys
- Bach

(5) Pumping stations

On the basic canal network of Hs DTD, there are six large pumping stations that serve to supply the canal with water, when this is not possible to a sufficient extent by gravity. They also serve to remove excess water from the canal network and to regulate the water level.

- Bezdán I
- Abyss II
- Bogojevo
- Becej
- Frog
- Pancevo

(6) Bridges

During the construction of the Hydrosystem DTD, many roads were cut, so 86 new bridges were built. Of these, 64 are road bridges, 21 are railway bridges, and one is a pedestrian bridge. The length of the bridge depended on the width of the canal, and the width of the bridge was determined by the road category. The lower edge of the structure is determined to allow navigation, or they are designed so that they can be moved such as electric, movable, steel bridges or wooden pontoon bridges.

4. HYDRO-NAVIGATION MEASUREMENTS ON THE DANUBE-TISA-DANUBE HYDROSYSTEM CHANNELS WITH RIVER FLEET VESSELS IN THE PERIOD FROM 2010 TO 2021

Navigation on the Banatska Palanka - Novi Becej canal

Navigation through this channel is possible along its entire length from PKM 0 to 147.3. There are three locks on this channel: "Kajtasovo" at PKM 8.7, "Botos" at PKM 85 and "Novi Becej" at PKM 147.

The "Kajtasovo" translation center was completed in 1979. It connects the main canal Banatska Palanka - Novi Becej with the Danube. It is part of the Kajtasovo hydronode together with the constitution of the same name. It has one double-winged and one segmental gate. Transports ships with a carrying capacity of up to 1000 t.

"Botos" lock was built in 1971. In the composition of the Botos hydronode, together with the constitution of the same name. It is located on the Banatska Palanka - Novi Becej channel. It provides navigation between the Central Banat and South Banat parts of Hs DTD. It has one sliding and one double-leaf gate. Transports ships up to 1000 t capacity.

"Novi Becej" translation facility was built in 1972. The task of this lock is to ensure navigation between the Tisza and the main canal Banatska Palanka - Novi Becej. It has two sliding gates. Transports ships up to 1000 t.

The dimensions of the locks are: length 85m, width 12m and depth 3m. The smallest measured depth of the channel is 1.7 meters. There are 19 bridges on this canal, and the smallest measured height of the free passage is 6.5 meters, under the gas pipeline bridge on PKM 55.

Navigation on the Begay Canal

Navigation through this channel is possible along its entire length from PKM 0 to 34.6. On this channel there is the "Stajicevo" lock at PKM 9.7. The "Stajicevo" lock was built in 1971 in Becej. It is part of the Stajicevo hydronode together with the Stajicevo watershed. It has two

sliding gates. It enables the connection between Tisa and the Banat part of Hs DTD. It can handle ships with a carrying capacity of up to 1000 tons.

Dimensions of the lock: length 85m, width 12m and depth 3m. The smallest measured depth of the channel is 3.2 meters. There are 10 bridges on this canal, and the smallest measured height of the free passage is 6.5 meters, under the railway bridge in Zrenjanin on PKM 26.

The largest populated place for basing ships is the town of Zrenjanin. In Zrenjanin, there is no organized place for mooring ships (there are no cleats, no connection to the city's water and electricity network), but the coast is walled along the entire length of the canal and is suitable for docking ships. Boats can be moored under the pedestrian bridge at PKM 27.8, where there is also a small pier for the boats of the nearby rowing club, where, with the approval of the VK managers, it is possible to get a connection to the water supply network.

Navigation on the channel Becej - Bogojevo

Navigation through this channel is possible along its entire length from PKM 0 to 90. There are three locks on this channel: "Becej" at PKM 0.2, Kucura at PKM 47.4 and "Bogoevo" at PKM 89.5 and one safety lock "Odzaci". The "Becey" translation house, which is thought to have been designed in Eiffel's office, was completed in 1896. It is located at the junction of the DTD canal with the Tisza. It is designed as a two-level gate with two sliding gates and one double-leaf gate (according to Tisza). It is the first lock in Europe that was powered by its own produced direct current. It has been out of use since 1975 and is protected as a cultural monument. The translation "Kucura" was completed in 1962. It enables navigation on the part of the Becej - Bogoevo main canal. It is located within the Kucura hydronode together with the Kucura constitution. It has two double gates. Transports ships up to 1000 t. The "Bogoevo" translation center was built in 1963. It is located at the junction of the Becej - Bogoevo canal with the Danube. Enables navigable connection between the Danube and navigable canals in Backa. It has two sliding "sunroof" gates. Transports ships up to 1000 t.

Odzaci Security Constitution was built in 1962. Its main task is to establish a second defensive line on the high ground of the Danube and Tisza watershed. It has two openings with a width of 16 meters each. The structure is closed with steel beam fasteners.

The smallest measured depth of the channel is 2.1 meters. There are 21 bridges on this canal, and the lowest measured height is 6.5 meters, under the railway bridge in Backi Gradiste on PKM 9.

Basing is possible in Srbobran, by bow connection on the left bank of the canal on PKM 27, the bank is low and dirt. There is no landscaped embankment for ships, trees nearby can be used.

Table 1. Overview of canal bridges and structures Becej – Bogojevo (*Source: Authors*)

1	Канал	ПКМ	Врста моста/устава	Путни правац	ВИСИНА МОСТА (цм)	ДУБИНА (м)
1	Канал Бечеј Богојево	1	друмски	Бечеј	610	2,3
2	Канал Бечеј Богојево	8,5	друмски	Бачко Градиште	630	2,5
3	Канал Бечеј Богојево	9	железнички	Бачко Градиште	605	2,1
4	Канал Бечеј Богојево	19,5	железнички	Надаљ	605	2,2
5	Канал Бечеј Богојево	25	друмски	Турија	720	2,9
6	Канал Бечеј Богојево	29	друмски	Србобран	670	2
7	Канал Бечеј Богојево	36	друмски	Ауто пут	660	1,7
8	Канал Бечеј Богојево	39,5	железнички	Врбас	650	2,2
9	Канал Бечеј Богојево	40	друмски	Врбас	620	2,3
10	Канал Бечеј Богојево	43,5	железнички	Магистрала	670	1,7
11	Канал Бечеј Богојево	47,4	друмски	Преводница Куцура	-	-
12	Канал Бечеј Богојево	52	друмски	Војни мост	670	2,9
13	Канал Бечеј Богојево	54	друмски	Савино Село-Деспотово	595	2,9
14	Канал Бечеј Богојево	55	железнички	Савино Село-Деспотово	612	3
15	Канал Бечеј Богојево	59	друмски	Косанчић	637	3,1
16	Канал Бечеј Богојево	67	друмски	Лалић-Руски Кретур	730	2,9
17	Канал Бечеј Богојево	72	друмски	Оџаци-Бачки Грачац	720	2,9
18	Канал Бечеј Богојево	73	железнички	Оџаци-Крушчић	760	3
19	Канал Бечеј Богојево	75	железнички	Оџаци-Бачки Брестовац	740	3
20	Канал Бечеј Богојево	77	друмски	Оџаци-Српски Милетић	690	3
21	Канал Бечеј Богојево	78	устава	Оџаци	690	2,9
22	Канал Бечеј Богојево	83	железнички	Каравуково-Богојево	700	3
23	Канал Бечеј Богојево	84	друмски	Каравуково-Богојево	700	3

Navigation on the Novi Sad - Savino Selo canal

Navigation through this channel is possible along its entire length from PKM 0 to 39.1. On this channel there is the "Novi Sad" lock at PKM 4.3. The "Novi Sad" translation center was completed in 1963. It is located 4.4 km from the junction of the Novi Sad - Savino Selo canal and the Danube. It is a part of the Novi Sad hydro node together with the constitution of the same name. It has one double-winged and one plunging gate. At this lock, the maximum unevenness between the Danube and the canal occurs (up to 9.1 m). Transports ships up to 1000 t. Dimensions of the lock: length 85m, width 12m and depth 3m. The smallest measured depth of the channel is 2.2 meters. There are 9 bridges on this channel, and the smallest measured height of the free passage is 6.1 meters, under the railway bridge in Novi Sad at PKM 7. At PKM 23.5, at the place of the old bridge, there is a narrowing of the waterway with a width of 17 meters.

Navigation on the Odzaci-Sombor canal

Navigation through this channel is possible along its entire length from PKM 0 to 27.8. There are two locks on this channel: "Srpski Miletic" on PKM 6 and "Sombor" on PKM 27. The "Srpski Miletic" lock was built in 1961. on the route of the Odzaci-Sombor navigable canal. Together with the constitution of the same name, it forms the Srpski Miletic hydronode. It has two double gates. Transports ships up to 1000 t. The "Sombor" prison was built in 1965. It connects different levels, i.e. it enables navigation between the Vrbas - Bezdán and Odzaci - Sombor canals. It has one plunging and one double-leaf gate. Designed to translate ships up to 1000 t. It can also work as a constitution. Dimensions of the lock: length 85m, width 12m and depth 3m. It is possible to base the ships near the village of Srpski Miletic on PKM 4. The smallest measured depth of the channel is 2.7 meters. There are 3 bridges on this canal, and the smallest measured height of the free passage is 7.21 meters, under the road bridge in Srpski Miletic on PKM 4.

Table 2. Overview of canal bridges Odzaci-Sombor (*Source: Authors*)

1	Канал	ПКМ	Врста моста	Путни правац	ВИСИНА МОСТА (цм)	ДУБИНА (м)
1	Канал Озаци-Сомбор	3	друмски	С.Милетић-Богојево	720	2,9
2	Канал Озаци-Сомбор	10	друмски	Дорослово-Сонта	735	2,9
3	Канал Озаци-Сомбор	20	друмски	Пригревица-Стапар	700	3

Navigation on the Prigrevica-Bezdan channel

Navigation through this canal is possible up to the main water catchment "Bezdan" at PKM 31.7 with the prior notice of the PUC "Vode vojvodina" in order to open the passage on the pontoon bridge at PKM 23. On this channel there is a safety dam "Kupusina" at PKM 12 and the main water catchment "Bezdan" on PKM 31.7. The "Kupusina" security structure was built in 1963 on the Prigrevica-Bezdan canal. The basic task of this constitution is the establishment of a second defensive line cut by the Prigrevica-Bezdan canal. In the event of a flood upstream of it, it takes over the role of the Bezdan water catchment system, in terms of the gravitational supply of water to Backa. It has two openings with a width of 16 meters each. The closing of the constitution is done with two sets of metal beam fasteners deposited in the houses on both sides of the constitution. The main catchment basin of Bezdan is the basin of the Bac part of HS DTD. It is located at the most upstream part of the Hydrosystem, at the junction of the Danube and the Prigrevica-Bezdan canal. According to the Constitution, water from the Danube is admitted to HS DTD with a flow rate of up to 60 m³/sec. Construction began in 1958 and was completed in 1960. The Constitution has three equal openings of 5 meters each, with segmental shutters measuring 5x4.2 meters. The smallest measured depth of the channel is 2.9 meters. There are 7 bridges on this channel, and the smallest measured height of the free passage is 7.3 meters, under the road bridge in Kupusina on PKM 9.

Table 3. Overview of canal bridges Prigrevica-Bezdan (*Source: Authors*)

1	Канал	ПКМ	Врста моста/устава	Путни правац	ВИСИНА МОСТА (цм)	ДУБИНА (м)
1	Канал Пригревица-Бездан	1	железнички	Сомбор-Пригревица	730	3,2
2	Канал Пригревица-Бездан	7	гасовод		-	3
3	Канал Пригревица-Бездан	9	друмски	Купусина-Апатин	730	3,1
4	Канал Пригревица-Бездан	10	железнички	Купусина-Апатин	740	2,9
5	Канал Пригревица-Бездан	13	друмски (устава)	Купусина-Апатин	740	3
6	Канал Пригревица-Бездан	23	понтонски	Б.Моношгор	-	3
7	Канал Пригревица-Бездан	31	друмски	Багина-Бездан	740	3,2

Navigation on the Vrbas-Bezdan channel

Navigation through this canal is possible from PKM 51.65 (the fork with the Odzaci-Sombor canal) to PKM 80.9 Bezdan") with the prior notification of the PUK "Vode vojvodina" in order to open the passage on the pontoon bridge on PKM 71. On PKM 72 there is the old constitution is 12 meters wide. Navigation through the channel from PKM 0 to PKM 51.65 is not possible due to the low height of the free passage for the ships of the River Flotilla. The "Bezdan" translation center was completed in 1856 and is the first facility in Europe where underwater concreting was applied. A concrete factory is organized on the construction site itself. Concreting lasted continuously day and night for 90 days. The portico had two pairs of double-winged gates at either end of the chamber. The pair of gates that corresponded to the water level at the moment the vessel passed through the lock was used. It connects the Vrbas-Bezdan canal with the Danube. In the period from 1995 to 2020, the lock of the lock was not in operation but served only for defense purposes against the high waters of the Danube. The smallest measured depth of the channel is 2.7 meters. There are 7 bridges on this canal, and

the smallest measured height of the free passage is 6.2 meters, under the railway bridge Sombor-Apatinna PKM 57.5.

The translator was put into operation on September 25, 2020. allows passage for ships of 500 tons and ensures a minimum draft depth of 3 meters. It has retained its authentic appearance as when it was built in 1856. year, so the gates are opened manually because it is protected as an industrial heritage.



Figures 5 and 6. Bezdán translation center after reconstruction

Source: Photographed on a voyage in 2021

Table 5: Overview of canal bridges Vrbas-Bezdan (*Source: Authors*)

1	Канал	ПКМ	Врста моста/устава	Путни правац	ВИСИНА МОСТА (цм)	ДУБИНА (м)
1	Канал Врбас-Бездан	55	друмски	Сомбор-Апатин	750	2,7
2	Канал Врбас-Бездан	57	железнички	Сомбор-Апатин	630	3
3	Канал Врбас-Бездан	57,5	железнички	Сомбор-Апатин	620	2,8
4	Канал Врбас-Бездан	68	друмски	Б. Моношгор	700	3
5	Канал Врбас-Бездан	71	понтонски	Б. Моношгор	100	3,4
6	Канал Врбас-Бездан	72	пешачки/устава	Б. Моношгор	740	3
7	Канал Врбас-Бездан	79,7	друмски	Сомбор	740	3

Navigation on the channel Backi Petrovac - Karavukovo

Viewing through this channel was possible in a length of 1.5 km and a passage was made under the Backi Petrovac - Novi Sad bridge. The width of the channel in this section is 35 meters, and the depth is about 2.3 meters. The width of the channel is a limitation for turning ships.

Sailing on the river Thames

A view of the Tamis river is possible up to PKM 3, at PKM 0.5 there is a safety post "Pancevo". The PANCEVO CONSTITUTION was built in 1973. at the mouth of the Tamis near Pancevo and is an integral part of the Pancevo hydronode. Hydronode Pancevo protects the coast of Lower Tamis from the negative effect of the stagnation caused by the HPP "DJerdap" dam. Pancevo allows for the separation of the waters of the Tamis and the Danube and maintains a controlled lower water level in the Tamis upstream of Opovo, enabling the passage of large waters of the Tamis. Ustava has three flow fields, the middle one is 24.5 meters wide and the two outer ones are 12 meters wide. The shutters are segmental.

5. CONCLUSION

Hydrotechnical and hydrological conditions on the canals of HS Danube-Tisa-Danube enable safe and secure navigation for ships of the River Flotilla on all canals on which surveys were carried out in the period from 2010 to 2021.

The research carried out in this period found that the locks enable the transfer of two ships of the River Flotilla, in one transfer it is possible to transfer three ships at the same time.

The height of the free passage under the bridges, the width and the measured depths on all channels of HS DTD III, IV and V categories allow for unhindered navigation by the ships of the River Flotilla

The speed on the HS DTD canals is limited by regulation to 8 km/h, in practice it is not possible to achieve a higher speed than 11 km/h, due to the limited width and depth of the canal. At a higher number of revolutions of the main engines, the load on their work increases and the large draw of water and the creation of waves.

All measurements and researches have confirmed that it is possible to safely navigate Hs DTD channels for ships with a displacement of up to 100 tons, a height of up to 5.40 meters and a draft of 1.20 meters. This enables the development of river transport to the cities on the canals (Becej, Novi Becej, Zrenjanin, Sombor...) and the increase of economic activity in the entire region.

The navigation of River Flotilla ships is enabled through the Hs DTD canals from Banatska Palanka (Danube river PKM 1075) to Novi Sad (Danube river PKM 1255), to Bogojevo (Danube river PKM 1367) and Bezdán (Danube river PKM 1425).

REFERENCES

Photos and notes from sailings for the purpose of reconnaissance of the Hs DTD channel in the period from 2010 to 2021.

Rosic, S. (2011). NAVIGATION IN INLAND WATERWAYS", Defense Media Center

THE WATER TRANSPORT DEVELOPMENT STRATEGY OF THE REPUBLIC OF SERBIA FROM 2015 TO 2025. (2015). "Sl. Gazette of the RS", no. 3/2015

Treasure book Hs DTD, Public water company Voda Vojvodina - Novi Sad.

<http://www.plovput.rs/>, Accessed: 15.06.2023.

<http://www.vodevojvodine.com/>, Accessed: 15.06.2023.

<http://www.hidmet.gov.rs/>, Accessed: 15.06.2023.

WAREHOUSE OPERATIONS SIMULATION FOR SAFETY IMPROVEMENT

Bojan Rupnik^{1a}, Tomaz Kramberger^{2b}

¹ University of Maribor Faculty of Logistics, Mariborska cesta 7, Celje, Slovenia,
bojan.rupnik@um.si

² University of Maribor Faculty of Logistics, Mariborska cesta 7, Celje, Slovenia,
tomaz.krabberger@um.si

Received: 6th September 2023

Accepted: 11th September 2023

Original scientific paper

Abstract: *Warehouse operations often include hazards due to relatively fast moving equipment. While there are multiple approaches to minimize hazards and increase safety in such environments, an alternative is to consider scheduling operations to further avoid potential threats. Spatial planning usually involves providing enough space for warehouse items, while transport routes and safety buffers can be neglected. This can lead to congestion effects within the warehouse which does not only decrease efficiency but can also increase accident occurrence. With performance usually being the highest priority, the operation organization is usually targeted to meet this priority and putting safety second. In this paper we cover an approach to organize the warehouse operation in order to increase efficiency by reducing congestion effects and thus increasing both safety and efficiency.*

Key words: *warehouse operation, forklift, discrete-event simulation, operation scheduling*

1. INTRODUCTION

Within the dynamic expanse of industrial environments, where the seamless and secure movement of materials constitutes a bedrock of operational efficiency, emerges the imperative presence of forklifts as indispensable workhorses. These mechanical entities navigate intricate tasks and expedite the unobstructed circulation of goods. However, commensurate with their pivotal roles, there arises an exigent demand for the augmentation of safety measures and strategic enhancements to forestall collisions and optimize overall performance. The compendium of scholarly papers at hand presents an exhaustive exploration of innovative paradigms and advanced technologies that coalesce to reinforce forklift safety while concurrently propelling operational efficiency to uncharted summits.

Spanning across diverse domains encompassing virtual reality, traffic engineering, automation, and the cutting-edge realm of ultra-wideband (UWB) technology, these scholarly

^a ORCID: 0000-0001-9983-1178

^b ORCID: 0000-0001-7656-5444

articles collectively illuminate pathways that endeavour to revolutionize the intricate realm of forklift operations. Each paper contributes a distinct facet to this multifaceted discourse, amalgamating into a mosaic of insights that collectively redefine the paradigm of forklift operations within the broader landscape of industrial endeavours.

Through immersive simulations, the initial paper delves into the nuanced arena of virtual reality, dissecting the situational awareness of forklift operators. It probes the depth of their perception vis-à-vis their surroundings and potential collision hazards. This vantage point augments the development of targeted training regimens and accident prevention strategies that are informed by a nuanced comprehension of operator cognition (Choia, et al., 2020).

The subsequent paper engenders a holistic perspective by amalgamating the domains of forklift safety, traffic engineering, and intelligent transport systems (ITS). Pioneering this holistic approach through an incisive case study, the paper explores the synergy inherent in harmonizing these facets. Such an amalgamation engenders improved traffic flow, augmented communication systems, and ultimately the cultivation of safer forklift operations (Horberrya, et al., 2004).

Embedded within this discourse, a comprehensive guidebook occupies a pivotal role, illuminating the arena of industrial traffic management and forklift safety. As a pragmatic resource, it proffers a roadmap for the delineation of optimal layout designs, implementation of traffic regulations, and formulation of communication protocols. This holistic guide holds the potential to evolve into an industry standard, reshaping safety practices across industrial complexes and akin settings (Larsson, et al., 2003). Moving into the domain of automation, the fourth paper ushers in a paradigm of automatic analysis of resource flows. Tracking the intricate trajectories of materials and forklifts within warehouse environments, this approach discerns zones prone to collisions. Empowered by data-driven insights, researchers and practitioners alike can instate preemptive strategies that mitigate risks, thereby shielding personnel and material assets from harm's way (Cantini, 2020).

Lastly, the fifth paper unveils the potential catalyzed by ultra-wideband (UWB) technology. The integration of UWB within forklift operations ushers in a new era of precision. Facilitating accurate positioning, collision evasion, and real-time tracking, this technology metamorphoses forklifts into astute tools that navigate with unparalleled precision, mitigating the prospects of accidents and magnifying operational finesse (Sun & Ma, 2017). Collectively, this assortment of scholarly contributions weaves a rich tapestry of ideas and innovations poised to advance forklift safety and efficiency. From harnessing the immersive capacities of virtual reality to reimagining traffic management through intelligent transport systems, each paper affords a distinct prism through which the intricate challenges of industrial landscapes are perceived. The embrace of innovation and interdisciplinary synergy emerges as a common underpinning, unveiling a realm of enhanced safety, augmented productivity, and accomplishments in the realm of forklift operations.

Simulating logistic operations is a widely used approach for many performance analyses including warehouse operations (Pawlewski, 2015). This paper uses the simulation approach to assess the safety aspect of forklift operations based on the planned organization and material flow.

2. WAREHOUSE SIMULATION

The presented paper covers a simulation of a potential warehouse organization. The warehouse is intended for supplying manufacturing of chemical products. As such the function of the warehouse is to store inbound materials from which the production lines are supplied. The materials are stored in EUR pallets in block storage. The entrance point of the warehouse

consists of a ramp for trucks from which the pallets are unloaded with forklifts and moved to storage locations within the warehouse. Due to the space constraints the pallets can occupy either a single slot or they can be stacked one on another, with a maximum of two pallets occupying being at the same slot. Overall, the pallets are doubly occupying a slot at approximately 50 %. With storage of inbound pallets presents the first process part, the second part consists of supplying the pallets to production lines. All movements of pallets are performed by forklifts. This scenario includes two priorities, which are supplying production lines on schedule and unloading cargo from the trucks to free the loading ramps.

2.1. Warehouse modelling

A virtual model of the warehouse was constructed in Flexsim (Flexsim Software Products, 2023) based on the planned warehouse layout. The 3D model includes the position of walls, objects such as elevator or conveyers and passages. A key part of the 3D model (Figure 1) includes the position of floor storages intended for pallet storage. The aim is to provide enough storage for a daily turnover of pallets, which covers around 400 pallets. The presented case differently sized storage locations to accommodate for the passages and maximized storage capacity.

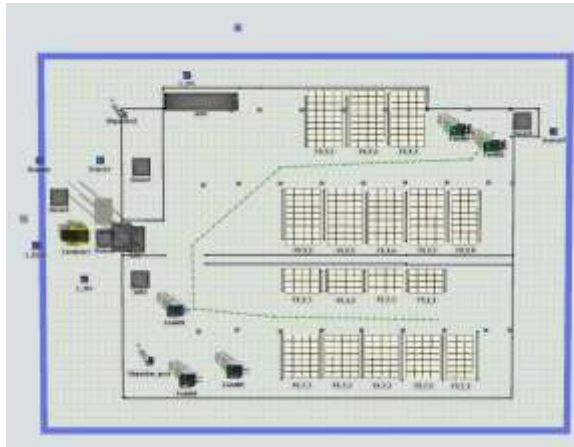


Figure 1. 3D model of the warehouse
Source: Authors

The 3D model includes any obstacles that cannot be passed by forklifts. The software allows for exact positioning of objects with set coordinates and dimensions. Moving the transport objects (forklifts) is done by the A* algorithm (Candra A, 2021), which finds the optimal path between the origin and destination location. For this purpose, the warehouse area is divided into nodes between which the transport objects can move. As the mathematically optimal path may lead to infeasible routes additional restrictions are included in the travel model, with the main one to avoid the forklifts to travel across the storage locations, which should only be entered from their direct front access. Another addition is the preferred path (marked green), which the forklifts will mostly follow except when their target object is close enough.

Another consideration during travelling is object collision. The software allows collision avoidance by constructing a circular buffer around the forklifts. In case of two forklifts coming to close one will stop, while the other will continue its travel until the proximity alert is finished. Proximity count and duration is a metric that can be used to assess the safety of forklifts during their operations with fewer proximity alerts and lesser proximity durations meaning higher safety.

2.2. Material flow

As stated previously, the main activities of the warehouse operations include unloading the cargo from the trucks, storing them at the floor storage locations and eventually supplying the materials to the production lines. In order to simulate the material flow it is necessary to consider: Pallet slots; Forklift specifications; Shift information; Inbound material flow; Production line requirement and Relocation requirements.

Table 1. Storage locations (*Source: Authors*)

Storage locations	Slots	Capacity
7	4x9	54
4	4x4	24
4	4x7	42
1	3x9	40
1	3x7	31

The storage locations (Table 1) show the available slots and approximate storage capacities given that it is possible to store two material pallets stacked one on the other at the same slot in half of the cases. The initial content of the warehouse is 400 pallets, which is the daily turnover.

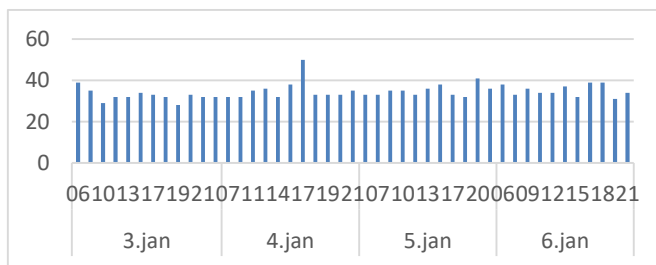


Figure 2. Inbound material quantities over time

Source: Authors

Expected inbound material pallets can be seen in Figure 2. The inbound arrivals are distributed over two shifts in which the forklifts unload the trucks and store them at available slots.

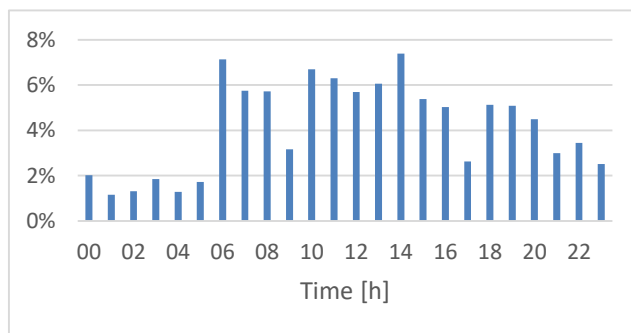


Figure 3. Distribution of production line requirements

Source: Authors

Along with storing materials in the warehouse the main priority is to provide a timely supply of the materials for the production lines. Figure 3 shows the distribution of pallet requirements for the production with visible spikes at the shift start and a low during the last shift.

2.3. Relocations

One of the main causes of congestions in the warehouse is the need for pallet relocations. The high variability of the production line requirements does not allow for an orderly storage of materials, which are consequently stored at a random slot with a few exceptions where materials of the same type are stored on adjacent slots. In the studied case such occurrences present less than 10% of required production orders and do not alleviate the problem. As the warehouse is mostly occupied at around 80% of capacity, supplying the production lines requires the time for finding the correct pallet, and in case of the pallet being stashed behind other, those need to be cleared in order to pick the ordered one. Depending on the depth of the ordered pallet this can lead to long delays, where pallets are intermittently stored in front of the storage locations or in case of many required relocations also in the transport route. While such relocation process takes place, other forklifts need to wait until the path is cleared again, and approaching such an event can increase accident occurrence.

Table 2. Probability of relocation needs (*Source: Authors*)

Relocations	4x4	4x7	4x9	Delay [min]
0	38%	24%	16%	0,00
1	23%	14%	10%	1,33
2	28%	16%	14%	2,67
3	6%	13%	11%	4,00
4	5%	13%	9%	5,33
5		8%	11%	6,67
6		6%	10%	8,00
7		3%	5%	9,33
8		1%	3%	10,67
9		1%	4%	12,00
10			4%	13,33
11			1%	14,67
12			1%	16,00

As shown in Table 2 the probability of relocation depends mainly on the depth of the storage location. The estimated delays cover the time of finding the picked pallet, removing all pallets stored in front of the required one, and storing all of the removed pallets back to the storage location. These times are considered for the average filled capacity of 80%. Each required relocation increases the probability of a safety issue.

3. SIMULATION RESULTS

Along with observing the schedules of production lines and truck arrivals, a key question is how many forklifts are required to fulfil all orders. We present two alternatives with the first having 4 forklifts in the first two shifts and 2 forklifts in the 3rd shift, the activities cover breaktimes. This solution is unfeasible as the available forklifts are not able to fulfil the requests for the production lines (Figure 4). Additionally, in this case the forklifts have practically no free time except for the breaks and are constantly on the either loading, unloading or moving, which occupies the workers to the maximum.

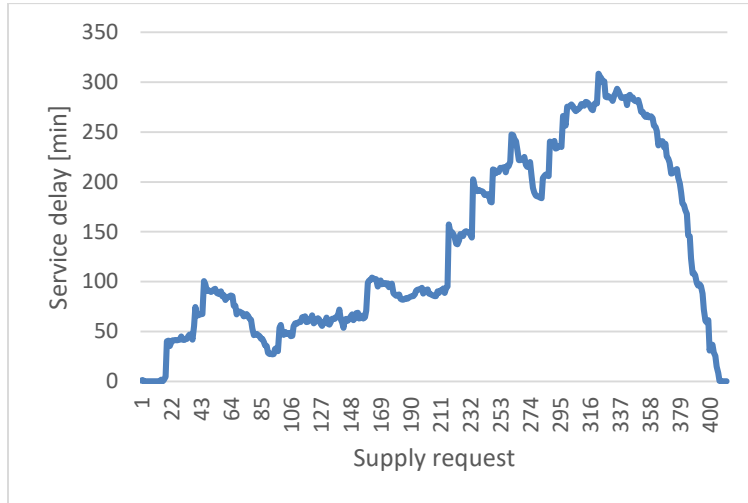


Figure 4. Delays for production lines in 1st scenario
Source: Authors

An alternative solution using 5 forklifts in the first two shifts and 3 forklifts in the 3rd shift can be seen in Figure 5.

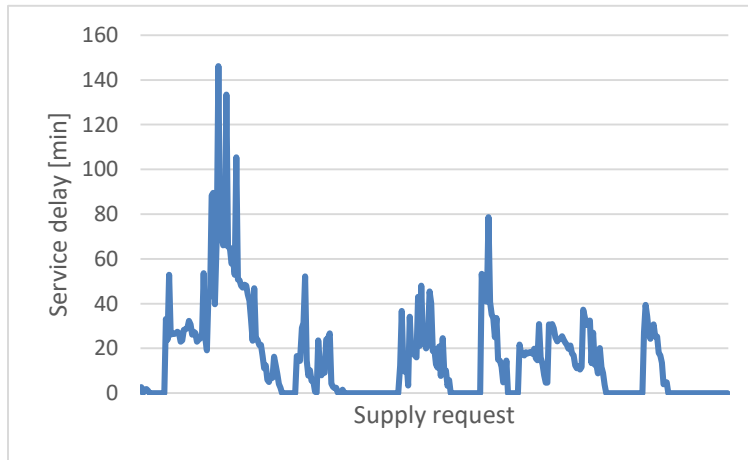


Figure 5. Delays for production lines in 2nd scenario
Source: Authors

This solution alleviates the forklifts throughout the day, while having spikes with delays they are still handled by the end of the work day. From the production point of view any delays are unwanted, meaning that both solutions are not feasible for fluent operations and alternative solutions may need to be explored

4. CONCLUSION

The presented simulation explores the option to analyse warehouse operation through simulation. From a production point of view both proposed solutions do not meet the requirements. Increasing the number of forklifts per shift does improve the warehouse performance, however it needs to be considered that this increases the number of near encounters between the forklifts and consequently the probability of accidents. The solution

to improve the situation both the performance as well as safety issue is by improving the overall organisation, meaning that the research should focus on effects of decreasing the supply in the warehouse and reorganize the inbound material frequency. Another option to increase safety is to designate forklifts to operate only in specific zones to avoid route mixing. The simulation approach provides an opportunity to analyse storage strategies and provide options to plan and improve organizational decisions.

REFERENCES

Cantini, A. F. (2020). Towards Forklift Safety in a Warehouse: An Approach Based on the Automatic Analysis of Resource Flows. *Sustainability*, 12, 8949.

Choia, M., Ahnb, S., & Seoc, J. (2020). VR-Based investigation of forklift operator situation awareness for preventing collision accidents. *Accident Analysis and Prevention*, 136, 105404.

Flexsim Software Procuets. (2023). Flexsim.

Horberrya, T., Larsson, T. J., Johnston, I., & Lambert, J. (2004). Forklift safety, traffic engineering and intelligent transport systems: a case study. *Applied Ergonomics*, 35.

Larsson, T., Horberry, T., & Brennan, T. (2003). *A Guidebook of Industrial Traffic Management & Forklift Safety*. Accident Research Centre Monash University Victoria 3800 Australia.

Sun, E., & Ma, R. (2017). The UWB based Forklift Trucks Indoor Positioning and Safety Management System. 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC). Chongqing: IEEE .

Pawlewski, P., (2015). DES/ABS approach to simulate warehouse operations. In *Highlights of Practical Applications of Agents, Multi-Agent Systems, and Sustainability-The PAAMS Collection: International Workshops of PAAMS 2015, Salamanca, Spain, June 3-4, 2015. Proceedings 13* (pp. 115-125). Springer International Publishing.

RISK ASSESSMENT DURING IMPLEMENTATION OF EXERCISES WITH MINE EXPLOSIVE ORDNANCE

Stefan Pusulic¹, Aleksandar Milic^{2a}

¹ University of Defense in Belgrade, Military Academy, Veljka Lukica-Kurjaka Street
Belgrade, Republic of Serbia, pusulicstefan@yahoo.com

² University of Defense in Belgrade, Military Academy, Veljka Lukica-Kurjaka Street
Belgrade, Republic of Serbia, milickm5@gmail.com

Received: 6th September 2023

Accepted: 11th September 2023

Professional paper

Abstract: *The paper investigates the importance and application of training soldiers with mine and explosive ordnance in order to reduce and manage risk. The army uses mine explosive ordnance to realistically simulate combat, with the aim of achieving a higher level of operability and reducing the risk to life. The training of soldiers in the placement and removal of mine explosive ordnance plays a key role in preparing members of the military for various military operations and tasks. Through the analysis, this paper concludes that the training of soldiers with mine and explosive ordnance has a significant potential to improve the ability and efficiency of the military in specific tasks. It also indicates the necessity of applying all available measures to reduce the degree of risk in working with mine and explosive ordnance.*

Key words: *mine and explosive ordnance, training, security measures*

1. INTRODUCTION

In the modern world where minefields, improvised explosive devices and similar dangers are a threat, training soldiers in the safe placement and removal of mine and explosive ordnance is a necessary and extremely challenging task in order to prevent and reduce losses and injuries.

The training of soldiers contributes to reducing the risk and increasing the efficiency of military operations, thus protecting the lives of soldiers and ensuring the achievement of military objectives.

The aim of the paper is to contribute to the understanding of the existence of risks when using mine explosives and explore the possibility of improving risk prevention in this area, thus ensuring that the training of soldiers is effective and safe.

^a ORCID: 0000-0002-2642-0340

2. THE TERM AND DEFINITION OF RISK

The concept of risk presents the combination of probability that a disaster will occur in a certain period of time and certain negative consequences. (Law on Disaster Risk Reduction and Emergency Management („Official Gazette of RS” No. 87/2018)).

Risk is an occurrence or situation that carries potential danger, harm or unwanted consequences. Risk can be present in various spheres of life, including health, investments, business and many other areas (Risk management and risk assessment methods, Prof. Dr. Aleksandra Kocic Arsic).

For the purpose of easier definition of risk, the following components can be used:

1. Identifying the potential hazard: Identifying the risk situation is a key element from which loss or damage can be derived.
2. Probability assessment: Assessing the likelihood of the risk occurring and the severity of the consequences.
3. Risk management: It involves the steps taken to reduce the consequence, this may include preventive measures, risk transversal or acceptance with awareness of the consequences.
4. Monitoring and auditing: Risk often changes over time, so it is important to monitor and reassess it to adapt risk management strategies.

Risk management is crucial in order to reduce potential damages and achieve the best possible success in various aspects of life and business.

In the military as in other organizations, there are different types of risks that can occur. The risks differ from the specific circumstances and engagement of the army on different tasks, and can vary from the loss of human life, disease, the risk of occupying territories during military conflicts, terrorist attacks, sabotage, espionage and other.

In the military, risk management is a key component of protecting resources (human lives and material assets), successfully completing tasks. The military, through strategies, invests significant efforts to ensure that risks are identified, minimized and managed in the best possible way in order to ensure the safety and efficiency of operations. For the purposes of the work, attention is focused on the risk associated with the implementation of exercises with combat mine and explosive ordnance.

3. TYPES OF EXERCISES WITH MINE AND EXPLOSIVE ORDNANCE

An important segment for the successful execution of various tasks of the military is the training of personnel for the execution of various tasks in combat operations. One of those tasks is working with mine and explosive ordnance (hereinafter: MEO). In order to ensure safe and secure work, it is necessary to train personnel in working with explosive mine explosives. The training is carried out by conducting exercises with mine and explosive ordnance.

Exercises with combat MEO are the most complex and highest form of training for soldiers, units and officers in handling explosives and means of activation when demolishing, creating and overcoming mine-explosive obstacles, using those means in exercises, when performing work on the organization of the territory and other tasks. (Instructions and training programs with MEO, 1995: point 6).

Exercises with MEO can be: demonstrations, exercises of individuals, exercises of units and experimental exercises. (Instructions and training programs with MEO, 1995: point 7).

The aim of the exercises is: to train personnel (soldiers, students) and units in the professional, safe and secure handling of activation and explosive substances during the demolition of elements and materials, in the creation and overcoming of mine explosive obstacles, with full compliance with the prescribed occupational safety measure when handling MEO. (Instructions and training programs with MEO, 1995: point 4).

Demonstration exercises with MEO represent the first meeting of personnel and units with these assets, which is why it is necessary to pay maximum attention to the preparation and execution of these exercises, especially measures to protect personnel and material assets. During the implementation of these exercises, attention is directed to the regularity of the work, the methodology of execution, as well as the presentation of the organization of the work during the realization of the exercise itself.

Exercises of individuals in handling MEO are carried out only after the soldiers and elders are well trained and practiced in handling the training equipment. Special attention is paid to safety measures at work when performing exercises.

Exercises of individuals in handling MEO are carried out with soldiers and elders and can be performed:

- Exercises where devices are used for detonating cord method of activating an explosive charge. This exercise is initial and carries the least risk of unwanted consequences.
- Exercises with the use of devices for the electric way of activating the explosive charge, a new level when performing the exercise, which causes an increase in the risk of unwanted consequences when performing such exercises.
- Exercises where the placement of combat anti-personnel and anti-tank mines is carried out. Such exercises require increased attention because the sensitivity during operation to the activation of certain mines is minimal.



Picture 1. Placement of an anti-tank mine
Source: Personal archive

Exercises of units with MEO include group, division, platoon, and company exercises. For the successful training of units, the previous good training of the individual in handling MEO is of crucial importance. The realization of these exercises represents the highest level of unit training in the use and activation of MEO.

Test exercises with battle MES are organized independently or as part of tactical and joint exercises in real conditions.

4. RISKS WHEN PERFORMING EXERCISES WITH MINE AND EXPLOSIVE ORDNANCE

Carrying out exercises with MEO in the military is a complex activity that holds significant risk. The risk when conducting exercises with MEO is reflected in the existence of a danger of serious consequences for the safety of soldiers and affecting the successful execution of the exercise.

The biggest risk relates to the safety of people's lives. Humanity is exposed to the risk of death or injuries that can cause amputations, burns, head injuries and more. In addition to the lives of soldiers, a great risk is also the possibility of damage to military equipment, vehicles or infrastructure, which can create unforeseen costs for repair or replacement.

Mistakes, which lead to risk, can also occur due to the carelessness of soldiers when using explosives or setting mines. Potential errors occur due to insufficient training that contributes to a good recognition of mine and explosive ordnance and how to use them. The risk arises if the soldiers were exposed to increased physical effort before the implementation of the exercises with MEO, so in those cases, those soldiers are prohibited from working with MEO. The appearance of high self-confidence can lead to reduced attention or skipping certain steps of the procedure in working with MEO and thus lead to risk. After a certain amount of time and working with the same means, soldiers develop "false confidence" (reflected in "excellent training for working with MEO") and curiosity for experimenting with MEO, which certainly leads to a dangerous situation. Experience and mentoring by professionals is an important decisive factor in how to react in a given situation.

When working with MEO, soldiers are under a lot of stress, which can affect their mental and emotional stability, but also their decision-making at the right time.

Atmospheric forces, the sudden appearance of animals or faulty equipment can also have a negative impact on exercise.

If injuries occur during exercises with MEO, it can have reputational consequences for the unit that implements them or for the entire military.

In order to act in the direction of risk reduction, the military implements a series of measures such as enhanced training of soldiers, controlled circumstances for the implementation of exercises, control and supervision during the use of MEO, as well as prescribed procedures on how to react in critical situations. It is of great importance to analyze each soldier separately, his capabilities and ways of reacting in a crisis situation, all with the aim of raising risk management to the highest level.

5. REDUCING RISKS OF THE IMPLEMENTATION OF EXERCISES WITH MEO

Reducing the risk of military operations is a constant challenge. By adopting optimal solutions and timely action on every form of unwanted consequence, the risk can be controlled or reduced.

In order to reduce and eliminate the possibility of risk, military organizations have prescribed procedures that contain measures to be taken: before exercises, during exercises and after exercises have been completed. In preparation for the implementation of exercises with MEO, the military plans and implements adequate training with training equipment, training each

individual to the prescribed standards that guarantee the recognition, handling, safe installation and removal of MEO. Identification of potential risks related to the exercise, the means of use and the terrain on which it is performed, should be an integral part of the preparation for the exercise. Based on that identification, safe zones and procedures for providing first aid and evacuation in case of injuries should be determined. Ensure that all participants in the implementation of the exercise understand their roles and responsibilities regarding safety during the exercise. It is important to inform the public about the time and place of the exercise with MEO and provide instructions on safe behavior.

During the implementation of the exercise with MEO, it should be ensured that the places where the MEO is installed are precisely determined and organized according to valid instructions, so that there are no unforeseen intrusions by other persons. It is forbidden to arbitrarily choose and determine the place where the contents of the training with MEO will be implemented. The obligation of the institution and the unit is to carry out a safety assessment for the specific area where the exercise is carried out. It must also define which exercises and with what amount of explosives can be carried out on that training ground. During the exercise, the soldiers must follow the instructions of the person in charge of their safety without question. The equipment used must be controlled and checked to guarantee its correctness. Exercises should be controlled by experts who can predict and react quickly in case of recognition of any risk. Clear communication and good cooperation of all exercise participants is a guaranteed success.

Reducing the risk after implementation of the exercise with MEO is also an important part of the overall process that guarantees the safety of soldiers and the environment. After the end of the exercise, a detailed inspection of the terrain should be carried out and it should be determined that there are no remaining MEO, in addition, all dangerous materials should be removed in order to ensure the safety of people who will move in that area after the exercise. Perform a detailed analysis of the exercise and, after identifying potential training deficiencies, take appropriate steps to prevent similar problems in the future. Continue with periodic training of all participants of the exercise so that procedures and procedures are not forgotten and thus increase the risk.

Soldier safety should be a priority at all stages of the exercise to minimize the risk of injuries and incidents.

All soldiers participating in exercises with MEO must be aware of the risks and responsibilities they bear during such exercises.

6. CONCLUSION

Training soldiers to deploy and remove MEO includes developing tactical thinking, teamwork and safety. Trained soldiers are able to effectively identify, handle and neutralize mine and explosive ordnance, which significantly reduces the risk to the lives of soldiers and the environment. Soldier training must be adapted to reduce risk and respond to new assets in the MEO domain. In addition, effective training allows soldiers to maintain a high level of capability and perform tasks with greater success.

Training soldiers with MEO is essential for the safety and effectiveness of all military operations. Constant improvement of training, adaptation to new threats are key steps towards the safety of soldiers' lives and the reduction of the risks associated with working with mines and explosive devices.

REFERENCES

Kocic Arsic, A., (1995). Risk management and risk assessment methods, Instructions and programs for exercises with mine explosive ordnance, General Staff of the Army of Yugoslavia.

Law on Safety and Health at Work ("Official Gazette of RS" No. 35/2023),

Labor Law ("Official Gazette of the RS" no. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 - decision of the US, 113/2017 and 95/2018),

Law on Disaster Risk Reduction and Emergency Management ("Official Gazette of RS" No. 87/2018).

http://ie.mas.bg.ac.rs/data_store/upload/22_terotehnolosko3.pdf, Accessed 10.08.2023.

CAMOUFLAGE, CONTENT OF RESOURCE PROTECTION, FOLLOWING EXPERIENCES FROM UCRAINE’S ARMED CONFLICT

Aleksandar Milic^{1a}, Dejan Blagojevic², Srdjan Kostic³

¹ University of Defense in Belgrade, Military Academy, Veljka Lukica-Kurjaka Street
Belgrade, Republic of Serbia, milickm5@gmail.com

² Academy of applied technical and preschool teacher studies, Aleksandra Medvedeva 20,
Nis, Republic of Serbia, dejan.blagojevic@akademijanis.edu.rs

³ University of Defence in Belgrade, Military Academy, Veljka Lukica-Kurjaka 33,
Belgrade, Republic of Serbia, srdjankostic36@gamil.com

Received: 10th September 2023

Accepted: 12th September 2023

Review paper

Abstract: Resource camouflage is one task that needs to be continuously planned and fulfilled. It is obtained in order to lower own losses, protection of secrecy of the combat forces deployment, hiding activities, real intentions, actions and other planned activities of Army’s units, in order to lower the effect of enemies actions and increasing of own forces protection capabilities.

Camouflage tasks are obtained by applying different means and technics, as well as technologies. Development of modern accomplishments in diverse science branches has found its application in forces protection. Positive – negative experiences from combat operations across the world during closer history considerably can be used as source of knowledge. Aside of current camouflage patterns on scene there are different materials enriched with new types of paints and coatings which reduce reflection during reconnaissance by technical appliances. With goal to diverse to false conclusions, new technically-technology solutions are applied by which the armored vehicles are camouflaged. The achieved effect is reflected in a completely different image on the screen of the means of observation in relation to what is being observed. At the same time with the development and application of new solutions, the analysis of the omissions in camouflaging is carried out, which leads to new knowledge, in the conditions of the application of new technical achievements in various combat utilities and systems. Application of new technical achievements imposed new tactical solutions that undoubtedly require new ways of applying camouflage measures.

Key words: camouflage, resource protection, models, drones

^a ORCID: 0000-0002-2642-0340

1. CAMOUFLAGE IN GENERAL

Planning and conducting various combat actions, in modern environment, can't be imagined without taking necessary force protection measures. Force protection, as part of content (influential) combat operations factor, "implicit preserving the combat potential of deployed forces in the combat zone, fighting against all enemy threats, natural and technological disasters and preventing actions" (Serbian Army's Doctrine, 2010). A part of force protection is camouflaging (Serbian Army's Doctrine, 2010). Because of that "it represents an integral and essential part of any operation" (Serbian Army's Operations Doctrine, 2012).

In general, about camouflaging has been written in textbooks (Rkman, 1988.; Saicic, 1971) in Serbian Army. This is an important topic for other countries as well, what the literature is about (Forbes, 2009; Ablor, 1999). Besides textbooks on topics of force protection through camouflage, vast number of papers have been published. Milic A. And others (2019) emphasize the necessity of constant monitoring of the level of development of reconnaissance techniques in order to timely harmonize camouflage measures with increasing the level of force protection (Milic, et al., 2019). Ravindran, A., Premkumar, A. (2014), present possibilities of active camouflage or adaptive camouflage that represents type of camouflage which adapts, often quickly, to the environment of the object (Ravindran & Premkumar, 2014). Qiao et al. (2021), present the results of research in the application of biomimetic adaptive materials that change color in stealth technology with the aim of developing a new generation of camouflage coatings for discoloration (Qiao et al., 2021). Ying et al. (2023) present application of infrared camouflage textile material that is soft and movable, which is the ultimate embodiment of infrared camouflage technology for individual soldiers (Ying et al., 2023).

Elias (2015) question of camouflage posts on high debate level of conducting physical, artistic and social camouflage not only in the battlefield but in a society as a whole (Elias, 2015). A., W., Houlbrook (1999), in his paper presents certain considerations about the need to develop capabilities, based on the development of technical means for image processing, in order to detect masked objects and assets in different terrain and environments (Houlbrook, 1999).

2. THE MATTER OF CAMOUFLAGE IN CONTEMPORARY CONDITIONS

Combat operations around the world in past decades point out all destructiveness of human creativity. The application of all technologies was not absent in situations where it is necessary to destroy human life or human assets. Modern technologies (and one of segments was presented in optoelectronic reconnaissance devices) affected the needs of developing camouflage assets focused on specific techniques and technologies. Movement represents greatest danger for camouflaged personnel and assets. To this end, a step beyond was taken and innovative performances were undertaken, presented through the development of modern technological and electronic means for deception during the movement of military equipment. The best example was given by British multinational company by the name of „British Aerospace – BAE“ (British air force). In 2011, at an exhibition in London, she presented her project in which she developed adaptive camouflage for combat vehicles that reduces the thermal signature and makes them invisible to infrared night vision devices. The technology "Adaptive" (<https://newatlas.com/adaptiv-ir-invisibility-cloak/19748/> accessed 17.07.2023. at 23:30) consists of hexagonal metal panels that are individually heated or cooled, allowing operators to completely blend in with their surroundings and imitate natural objects or other vehicles such as harmless cars. The company announced plans to use "Adaptive" for air and maritime vehicles. If succeeded, this camouflage technology will revolutionize the art of war with new tactics and infiltration operations behind enemy lines. Although "BAE" has taken the lead, it is not the only company focused on development of adaptive camouflaging systems.

Izrael also experiments with “OIRAP” system for protection of invisible armor developed by the “ELTECH” (The red fox). Military research and development centers in USA and “DARPS” agency also work on similar projects (<https://www.youtube.com/watch?v=QKfVYVuxiQ8> accessed 17.07.2023. at 21:10).

The matter of camouflage can be interpreted from different aspects. This is also shown by looking at the degree of masking of the vehicle by removing the shadow created by the vehicle during movement (Yangping et al., 2017). The degree of achieved camouflage and its influence in conducting war is always under close observation (Pomerleau, 2017) and assumptions are given of application of modern technical innovations in battlefield (Rayment, 2011). Current camouflage possibilities by standard issued assets are continuously analyzed with the tendency of their improvement (Michalis et al., 2017), and performs an analysis of the capabilities of existing assets in relation to the impact of the environment and technical assets (Fennell, et al., 2018; Lin et al., 2019; Talas et al., 2018; Ershadi et al., 2018).

The available published content indicates that the issue of camouflaging is approached very studiously and constant analyzes are carried out with the tendency of constant development and application of various means and techniques. The last examples indicate that in the recon tasks mini and micro drones are used that are equipped with high sensitive optoelectronic additions for collecting information from environment.

3. EXPERIENCES ON CAMOUFLAGE TASKS DURING COMBAT OPERATIONS IN UKRAINE

Special military operation in Ukraine and its consequences gave entirely new dimension in matters of camouflaging units. When one tries to look at the reality, one encounters a great wall of silence due to the strong blocking of sources on the Russian side. It is precisely for this reason that it is necessary to look critically at the presented contents that are available.

From analyzing of available materials (footages, videos and printed materials) conclusion can be made that there have been many failures in conducting camouflage precaution measures. One of the reasons relies on a fact that some of the senior staff disobeyed basic tactical principles.

Regardless on existence of forest terrain and constant pointing out on possibilities for camouflaging units in a way to enter the woods and park under the trees, the results show the opposite. It is forgotten to avoid grouping of assets. It is forgotten that we are in 21-st century, the era when reconnaissance is conducted by unmanned aerial vehicles - drones and from a height of several tens to several hundred meters. Recorded material is transferred in real time to the required addresses. Therefore, large number of destroyed techniques is not surprising (Figure 1).



Figure 1. Destroyed armored combat vehicles on a bank of Siverski Donec river 12.05.2022.
 Source: Ukrainian Airborne Forces Command/Reuters, <https://www.voanews.com/a/russia-takes-losses-in-failed-river-crossing-officials-say-/6570694.html>

Forced water obstacle crossing is combat operation that is conducted in extreme need. In case it is necessary to implement this activity, it is necessary to ensure a strong anti-aircraft defense system or air superiority. If the mentioned items have been complied with, the planned activity can be started. What is forgotten in modern conditions is the necessity of applying camouflage discipline, which also relies on respecting the plan of crossing the water obstacle. The consequences of not complying with the above are catastrophic. With disrespect of camouflage measures comes the reveal of point of crossing over water obstacle. In this situation it is not important if the water obstacle crossing is forced or not. An additional aggravating circumstance that led to huge losses is failure to follow the plan for crossing the water obstacle. Due to the unplanned bringing of units to the boarding ramp and crossing area, there was a larger number of units and assets than planned. Again, thanks to acquired information in real time, a strike was made from a distance and the effects are visible in Figure 2.



Figure 2. Destroyed pontoon bridge on bank of Siverski Donec river 12.05.2022.
 Source: Ukrainian Presidential Press Office via AP, <https://www.timesofisrael.com/ukraine-inflicts-huge-losses-on-russians-during-failed-river-crossing-officials-say/>

Organized units movement during combat operations always represents high risk activity. Precisely because of all the experiences during combat actions, it is necessary to approach the organization of this activity extremely seriously. Failure to take all necessary measures of camouflage discipline leads to results that are represented by the consequences on Figure 3.



Figure 3. Destruction of assets in line

Source: Ukraine Military Claims It Blew Up A Bridge Destroying Russian Convoy, Amit Chaturvedi, 14.04.2022., <https://www.ndtv.com/world-news/ukraine-military-claims-it-blew-up-a-bridge-destroying-russian-convoy-2888420>

It is pointless to talk about the consequences. The photo clearly shows that there was no camouflage of the vehicles, no account was taken of the distance between the vehicles, the movement was organized without prior planning of potential hiding places to protect the vehicles. Experience from combat operations dictates that movement in the operation zone must be carried out in conditions of low visibility, in jumps or adjusted to terrain conditions in order to create masking conditions. An additional example of not learning about possible consequences from examples is also shown in the Figure 4.



Figure 4. Failure to comply with prescribed measures of camouflage discipline and consequences

Source: Specialist Ukrainian drone unit picks off invading Russian forces as they sleep <https://www.thetimes.co.uk/article/specialist-drone-unit-picks-off-invading-forces-as-they-sleep-zlx3dj7bb>

The layout of the marching column was copied from school textbooks. It is the non-observance of the measures that leads to the situation that the stop is made in an open area, without removing the vehicles from the road and masking them. Therefore accomplished success of the opponent and suffered casualties (in manpower and material goods) is no surprise.

It is to be expected that more attention is paid to the issue of camouflage during the possession of firing positions. Especially when it is known that there are artillery or artillery-rocketery

units. The positions of the mentioned units, due to their sensitivity to the action of aviation or artillery (through contrabattling), must be very well protected and camouflaged in order to make it difficult to spot them. The required works were not complied with, as evidenced by Figure 5.



Figure 5. Artillery positions established in Talakivka, north of Mariupol, Ukraine,
Source: Satellite image ©2022 Maxar Technologies. <https://www.businessinsider.com/how-russia-is-waging-its-war-with-artillery-in-ukraine-2022-7>

The material just presented indicates all the recklessness and audacity of those who should take care of entrusted human lives and technology. If an attempt were made to find "some justification" through the size of the position and the extent of camouflaging works, the question arises as to what happens to smaller positions that do not require extensive camouflage works. We come to a devastating fact that no one bothers with this issue. Pictures available on the internet show that demand in camouflage is not even considered (Figure 6). It imposes question if the participants of combat operations are aware of danger that carries the fact that the units' positions in the 21st century MUST be camouflaged with outmost care and dedication. Any revealing sign can lead to diminish large number of personel (entire unit).



Figure 6. Fortified positions of infantry units
*Source: Russian forces in Crimea brace for possible Ukraine counteroffensive;
<https://www.pbs.org/newshour/world/russian-forces-in-crimea-brace-for-possible-ukraine-counteroffensive>; 11.04.2023.*

That attention must be paid to the issue of masking military interesting objects during their construction is a hard to understand fact. Especially for those who haven't faced the terrible of war. In recent decades, there is no mention of reconnaissance by satellite. The attention is focused on unmanned aerial vehicles and drones. However, it is not always so simple to ignore. The fact is that military interesting objects are often indepth of countries territory, so satellites are used for reconaissance of such areas. Therefore, it is not surprising that images of objects

that represent very interesting targets have emerged. Military industry facilities that "should" be highly secured (Figure 7).



Figure 7. Works on the construction of a facility for portable rocket launchers

Source: Hans Kristensen <https://fas.org/blogs/security/2021/02/plarf-jilantai-expansion/>

Modern technology is very useful. However, of its dangers are only to be heard. It is precisely the desire to organize life more easily and enjoy the benefits offered by the modern world, which is often identified with the use of mobile phones or global positioning systems, that can be a great danger. Those appliances leave digital fingerprints or locations where they have been or if they are on the move. Such data can reveal information that can be used usefully.

It is a common craze to use mobile phones during running (to maintain fitness) to listen to music, monitor certain health parameters. No one is asking what is happening with collected data and where are they sent. Precisely such data helped to locate and draw the area of a base camp of a unit stationed outside of its own country (Figure 8).



Figure – 8. The footprint of the mobile phone's movement in space

Source: Fitness app Strava lights up staff at military bases, 29.01.2018.

<https://www.bbc.com/news/technology-42853072>

Clearly the traces are marked to where some phones were moving and picture for itself points that it is some sort of camp which includes runways and appropriate facilities. Also, conclusion can be made of boundaries of the camp, because it is not logical that no cell phone has moved outside the outlined circle.

This example that demonstrates “the danger” of applied GPS devices that are installed in vehicles lately for safe tracking are best shown in Figure 9.



Figure 9. Reading the vehicle's marching route during reconnaissance
Source: Fitness app Strava lights up staff at military bases, 29.01.2018.
<https://www.bbc.com/news/technology-42853072>

In the picture, you can clearly recognize the march route that the vehicle took during the reconnaissance of a certain area. The trace of movement is what shows the routine and therefore enables planning of actions over units that move on that track. Therefore it cannot come as a surprise the frequency of applying various explosive devices on certain parts or traces of roads.

4. CONCLUSION

Camouflage, as part of force protection, proves its importance every day. It is impossible to divide matters of camouflage to the times of peace and times of war. Data are being collected constantly, so therefore it is necessary to constantly apply measures of camouflage discipline. Besides applying camouflage measures it is necessary to constantly monitor development of reconnaissance appliances and their capabilities. It is the only way for creating the possibilities for adequate solutions on how to protect one's resources.

Development of paints, coatings, materials and technologies indicate that it is necessary for the man to change. To begin with, it is necessary for the members of the army to wake up and understand the limits of human irresponsibility and stupidity. By comprehending the reality conditions are made for lowering casualties.

As a possible solution, the possibility of using models to mislead the enemy arises. The next possibility is to consciously change certain tactical principles and clichés of behavior (that the assets are parked in the meadow in a line). Changing principles of units' engagement is conditional to contemporary reconnaissance assets and long range operations.

REFERENCES

- Abler, Th., (1999), *Hinterland Warriors and Military Dress: European empires and exotic uniforms*, Oxford: Berg, 4.
- Serbian Army's Operations Doctrine (2012), Media centar "Odrbrana", Belgrade.
- Serbian Army's Doctrine, (2010), Media centar "Odrbrana", Belgrade.
- Elias, A. (2015). *Camouflage Cultures: Beyond the Art of Disappearance*. Sydney University Press. ISBN 978-1-743324-25-7.
- Ershadi, N., Y., and others, (2018), Robust vehicle detection in different weather conditions: Using MIPM, <https://doi.org/10.1371/journal.pone.0191355>

- Fennell, J., G., and others, (2018), Optimising colour for camouflage and visibility: the effects of the environment and the observer's visual system, www.researchgate.net/publication/327925961, DOI: 10.1101/428193
- Forbes, P., (2009), *Dazzled and Deceived: mimicry and camouflage*, London: Yale University Press.
- Houlbrook, A., W., (1999), The Development of an image manipulation facility for the assessment of CCD, *This Proceedings*.
- Lin, C., J., and others, (2019), Optimization of color design for military camouflage in CIELAB color space, *Color Res Appl.*; 1–14. <https://doi.org/10.1002/col.22352>
- Michalis, C., and others, (2017), Optimal background matching camouflage, *Proc. R. Soc. B* 284: 20170709. <http://dx.doi.org/10.1098/rspb.2017.0709>
- Milic A., Randjelovic A., Radovanovic M., „Camouflage in resource protection function“, 5th International Scientific and Professional Conference “Security and Crises Management–Theory and Practice SeCMan 2019”, pp. 99-105, ISBN 978-86-80692-04-3.
- Pomerleau, M., (2017), Electronic camouflage will be the new war paint, www.c4isrnet.com/electronic-warfare/2017/09/21/electronic-camouflage-will-be-the-new-war-paint-says-marine-intel-official/
- Qiao, Y., et.al. (2021) “Research Progress of Bionic Adaptive Camouflage Materials”, *Frontiers*, Volumen 8/2021, <https://doi.org/10.3389/fmats.2021.637664>.
- Ravindran, A., Premkumar, A. (2014), “Camouflage technology”, *International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)* ISSN: 0976-1353 Volume 8 Issue 1.
- Rayment, S., (2011), Invisible tanks could be on battlefield within five years, <https://www.telegraph.co.uk/news/uknews/defence/8247967/Invisible-tanks-could-be-on-battlefield-within-five-years.html>
- Rkman, I., (1988), *Maskiranje*, VIZ, Beograd;
- Saicic, S. (1971), *Camouflaging*, Military Publishing House, Belgrade.
- Talas, L., and others, (2018), Evolving optimum camouflage with Generative Adversarial Networks, www.researchgate.net/publication/327984758, DOI: 10.1101/429092
- Yangping, W., and others, (2017), Analysis on Removal of Vehicle Shadow Based on Edge Feature and HSV Color Space, *Journal of Engineering Science and Technology Review* 10 (5), pp.84-89, DOI: 10.25103/jestr.105.10
- Ying, S., Bin, Y., Zao,X., (2023), Research status and development of infrared camouflage textile materials, <https://journals.sagepub.com/doi/abs/10.1177/00405175231170323>.

CHARACTERISTICS AND CONSEQUENCES OF NATURAL DISASTERS IN THE TERRITORY OF THE REPUBLIC OF SERBIA

Nikola Vukojevic¹, Stefan Tomic², Aleksandar Petrovic³

¹ University of Defense, Military Academy, Veljka Lukica Kurjaka 33, Belgrade, Republic of Serbia, nikola_vukojevic@ymail.com

² University of Defense, Military Academy, Veljka Lukica Kurjaka 33, Belgrade, Republic of Serbia, stefan.tomic1991@yahoo.com

³ University of Defense, Military Academy, Veljka Lukica Kurjaka 33, Belgrade, Republic of Serbia, ale_petrovic@live.com

Received: 10th September 2023

Accepted: 12th September 2023

Professional paper

Abstract: *Natural disasters are the cause of great damage, they complicate and partially or completely prevent the functioning of various systems in society. As a result of natural disasters, human lives, material and cultural goods, infrastructure of various purposes are lost, while financial losses are measured in tens of millions of euros. Only in the 21st century, Serbia was affected by a large number of natural disasters that claimed human lives and caused large financial losses. Some of the most destructive natural disasters that have affected Serbia and for which there are real indications that they will be repeated in the future are earthquakes, floods and fires. A characteristic of all of them is that they do not occur at specific time intervals, but the areas where floods or forest fires can occur are well known, also the areas affected by earthquakes cannot be determined with certainty because in the previous 100 years, many devastating earthquakes occurred in different parts of Serbia. The consequences of these disasters are as great as the investments to eliminate them, and recovery from such events takes a long time.*

Key words: *natural disasters, earthquakes, floods, fires, consequences*

1. INTRODUCTION

Since their first ever communities, people have encountered natural disasters and other misfortunes that they could not explain. They often tried to explained these phenomena as the desire of a supernatural force, which manifested itself as a consequence of people's bad behavior. Disasters, both natural and those caused by technical - technological and other accidents, in recent decades represent an increasing threat to the life and work of people all over the world. Natural disasters in all their forms are the cause of great damage, they complicate and partially or completely prevent the functioning of various systems in the society. As a result of natural disasters, human lives, material and cultural goods, infrastructure of various purposes are lost, while financial losses are measured in tens of millions of euros.

This paper deals with some of the most devastating natural disasters that have affected the territory of Serbia and for which there are real indicators that they will be repeated sometime in the future. Earthquakes, floods and forest fires are the natural disasters that take the most lives and cause the greatest financial and material losses. A characteristic of all of them is that they do not occur at specific time intervals, but the areas where floods or forest fires can occur are well known. Part of the work also refers to the consequences of these natural disasters. Since the floods in Obrenovac in 2014 or the earthquake in Kraljevo in 2010, the affected citizens and the Republic of Serbia have been recovering for a long period of time.

2. THE CONCEPT OF NATURAL DISASTERS

"Disasters are natural calamities or technical-technological accidents whose consequences threaten the safety, life and health of a large number of people, material and cultural goods or the environment on a larger scale, and the occurrence and consequences of which cannot be prevented or eliminated by the regular action of competent authorities and services" (Law on Disaster Risk Reduction and Emergency Management). In Serbian legislation, the concept of elemental disasters is equal to the concept of natural disasters, which is not often the case with the legislation of other European or world countries. Natural disasters are defined in the Law on Emergency Situations as "events of hydrometeorological, geological or biological origin, caused by the action of natural forces such as earthquakes, floods, storms, extreme temperatures, epidemics of infectious diseases... which can threaten the health and life of people or cause damage on a larger scale" (Law on Emergency Situations).

Natural disasters are part of the ecological sphere in which we live. Floods, hurricanes, storms, earthquakes play an important role in regulating the larger natural systems on which we all depend. Attempts to physically modify these systems often have serious consequences including increased vulnerability to hazards and post-disaster damage. Natural disasters are sudden and seemingly inevitable, but natural disasters can also occur as a result of events that take place over a number of years. Many geomorphological hazards that progress slowly (drought, soil erosion and degradation, desertification, rising of the sea levels, loss of biodiversity etc.) can have long-term catastrophic results and cause natural disasters with serious consequences (Mladjan, 2015).

Natural disasters lead to financial, environmental and human losses. The loss depends on the vulnerability of the affected systems and the readiness of the state administration to respond to the challenges. In practice, the terms natural phenomenon and natural disaster are often confused. "Natural phenomena are extreme climatological, hydrological, geophysical and other processes, which do not pose a threat to man and his property" (Mladjan, 2015); while natural disasters are phenomena that disrupt the stability of natural processes and can cause great damage to society and its parts. A strong earthquake in uninhabited parts of the world or fires that hit grassy or forested areas and do not directly affect human life and work do not represent a natural disaster but instead a natural phenomenon.

Natural disasters, as harmful events for people, their material goods and the environment, occur in different spheres of the country. According to the location of occurrence, natural disasters can be divided into the following categories: lithospheric (earthquakes, volcanic eruptions, landslides, rockslides, soil collapses and dangers from outer space); hydrospheric (floods, tsunamis, snow avalanches); atmospheric (intense precipitation, extreme temperatures, stormy winds, electric discharges, frost, ice, fog and droughts) and biospheric (epidemics, epizoonoses, epiphytonoses, forest fires) (Mladjan 2015).

2.1. Lithospheric disasters

The word lithosphere is derived from the Greek words "lithos" meaning stone and "sphaira" meaning ball (envelope) (vokabular.net/litosfera/). In translation, the lithosphere is the rocky or solid covering of the Earth or the Earth's crust. It is precisely in this part of the Earth that certain phenomena and processes occur that cause some of the most devastating natural disasters, namely earthquakes, volcanic eruptions, landslides, rockslides, and soil collapses. Dangers from the cosmos such as meteor or asteroid impacts are classified as lithospheric disasters because these celestial bodies are very similar to the Earth's crust in terms of their characteristics and composition.

Earthquakes, volcanic eruptions, landslides, rockslides and soil collapses are natural phenomena that occur on earth every day and are caused by phenomena that occur in the Earth's crust. These natural phenomena, if they occur in populated areas, cause great material damage, loss of human life, and thus we are talking about natural disasters. Earthquakes, as the cause of natural disasters, take by far the most human lives, as much as 47%, and are also responsible for the greatest material losses, as much as 35% (Mladjan, 2015).

2.2. Hydrospheric disasters

Hydrosphere is a word derived from the Greek words "hydro" meaning water and "sphaira" meaning ball (sheath) (vokabular.net/hidrosfera). In translation, the hydrosphere is the water envelope of the Earth. The water envelope of the Earth includes all bodies of water on earth: oceans, seas, lakes (natural and artificial), rivers, ponds... It is precisely these forms of water bodies that cause natural phenomena that can be characterized and categorised as disasters when they threaten or cause loss of human lives, material and cultural goods. According to the processed data, in the period from 1900 to 2010, as many as 200.000 human lives were lost by floods in the world (Mladjan, 2015). A devastating tsunami is a rare natural disaster and is most often caused by a strong earthquake. One of the most devastating recorded tsunamis to hit the world happened in 2004. in Southeast Asia. It was caused by an earthquake with a magnitude of 9 on the Richter scale, and waves of 10 meters in height caused catastrophic material damage, while the death toll was around 320.000 (Mladjan, 2015).

2.3. Atmospheric disasters

Atmosphere is a word derived from the Greek word "atmos" meaning air and "sphaira" meaning ball (envelope) (vokabular.net/atmosfera/). The atmosphere represents the air or gaseous envelope of the Earth. Many human activities are connected and dependant on the events unfolding in the atmosphere. Atmospheric disasters are: droughts, extreme temperatures, large amounts of precipitation, stormy winds and electrical discharges. Atmospheric disturbances that cause natural disasters do not always have to result in lost lives. The loss of human life is most often caused by droughts, extremely high temperatures and large amounts of rainfall that cause floods. Such was the flood in Obrenovac in 2014. which was caused by extreme rainfalls, or large-scale fires in Serbia from 2012. which caused severe droughts and extremely high temperatures.

2.4. Biosphere disasters

Biosphere is a word created from the Greek words "bios" and "sphaira", which includes all life on Earth, all plant and animal life (vokabular.net/biosfera/). Events caused by diseases of inhabitants, animals and plants are called biospheric (biological) disasters (Mladjan, 2015). The consequences of these disasters affect only the living world and are manifested by illness and death. They are divided into epidemics (the appearance of a disease in a number that exceeds its usual frequency in the population), epizoonoses (diseases of domestic and wild animals, which can affect a large number of animals in a large area) and epiphytonoses (sudden plant diseases take on the character of a natural disaster, because they cause great material

damage and endanger human lives). Plant diseases are particularly dangerous if the disease affects large areas under crops, which reduces the amount of food produced and, which in turn causes increased hunger that finally causes a rise in hunger-induced deaths, especially in poverty-stricken countries.

3. CHARACTERISTICS OF NATURAL DISASTERS IN THE TERRITORY OF THE REPUBLIC OF SERBIA

The geographical position and relief characteristics of Serbia are very favorable, and Serbia is rich in natural resources. More precisely we are talking about great natural riches of rivers and lakes, forests and mountains.

A large number of rivers, which in the northern parts of the country are also important waterways, often due to the features of the relief, the river bed, but unfortunately also due to the insufficient arrangement of the river banks, cause large floods, which take human lives and cause great financial losses. The wealth of coniferous, deciduous and mixed forests brings great benefits to Serbia, but also the constant danger of large forest fires. As a country located on the Balkan Peninsula, which is defined as a fragile area, in its past it had to fight with devastating earthquakes, which also claimed human lives.

3.1. Earthquakes

Earthquakes belong to the group of geophysical and lithospheric disasters and are very frequent, with most of them being of lower intensity. Stronger earthquakes can cause great material damage and serious consequences for people, by creating cracks in the Earth's crust, shaking the ground, causing floods and release of hazardous substances. Earthquakes as natural disasters are caused by the sudden stacking of large slabs of rock along fractures within the earth (Cvetkovic 2020). During an earthquake, violent movements cause waves and cause incredible destruction when they reach the earth's surface. These violent tremors can last for several minutes, destroying buildings, bridges and most other critical infrastructure facilities. The higher the population density and the number of endangered buildings and infrastructure, the greater the possibility of a disaster.

Analysis of seismic activities clearly shows that Serbia belongs to a region characterized by moderate (average) seismic activities, taking into account their number, frequency and intensity. Also, there is an irregular distribution of epicenters, which makes it much more difficult to distinguish seismic faults. In the period from 1900. to 1970. earthquakes of higher intensity were registered in the areas of Rudnik (mountain), Lazarevac, Juhor (mountain), Krupanj, Jagodina, Vranje and Vitina, while after 1970. three earthquakes of moderate intensity were registered in the areas Kopaonik, Mionica and Trstenik (Cvetkovic 2020).

Earthquakes of up to 6.1 on the Richter scale have occurred on the territory of Serbia. Considering the sheer amount of their energy, and considering the unfavorable invulnerability of the built infrastructure, such earthquakes can be very destructive. In the previous 100 years, the territory of Serbia was hit by about 400 earthquakes of strong and moderate intensity and about 6.000 of weak intensity. Kopaonik, Arandjelovac, Valjevo, Kosovo and Metohija (Gnjilane and Vitina) and Vranje are the parts of Serbia with the most seismic activity and the parts where strong and medium-intensity earthquakes have occurred and where there is a high possibility of earthquakes in general. (Assessment of the risk of disasters in the Republic of Serbia 2017).

3.2. Floods

Serbia has a favorable geographical position. Its waterways, especially the Danube River, have exceptional potential (Disaster Risk Assessment in the Republic of Serbia 2017). The largest

rivers are transit watercourses, which also have great water management importance. However, in the basins of these rivers, lie the biggest water management problems, such as floods, sometimes strong soil erosion with the appearance of ravines and flash floods (Assessment of the risk of disasters in the Republic of Serbia 2017). According to the data of the Water Management Foundation of the Republic of Serbia, "close to 1.6 million hectares, of which about 80% is arable agricultural land, is at risk of flooding." There are more than 512 large settlements, 515 industrial and other economic facilities, 680 km of railways and about 4.000 km of roads on potentially threatened areas" (Assessment of the risk of disasters in the Republic of Serbia 2017).

Taking into account the territory of the Republic of Serbia, it can be said that the degree of threat to the population and material assets is not the same throughout the territory. The largest flood areas are located in the Tisa (2.800 km²), Sava (2.243 km²), Velika Morava (2.240 km²) and Danube (2.070 km²) river valleys (Cvetkovic 2020). In the previous ten-year period, numerous floods were recorded on the territory of Serbia. Small drops in the river beds, morphological characteristics of the terrain and wide alluvial plains cause frequent flooding in the Tisa valley. There is no doubt that various anthropogenic influences contribute to the increase in the risk of floods in Serbia. According to the size of the threatened areas, in second place, after Vojvodina, is the right bank of the Sava, and then the areas in the Morava basin, along the right bank of the Drina, in the Belo Drima, Kolubara, Sitnica, Timok, Binacka Morava and Lepenc basins. In Serbia both small and big rivers pose a threat of flooding. Floods can be caused by rainfall and snow thawing, or by the coincidence of high-water levels or caused by landslides and water dam destructions. (Cvetkovic 2020.).

3.3. Forest fires

Fires are a very common occurrence in modern society and are not considered disasters but extraordinary events, unless they cause more serious human and material losses. Fire, as a frequent and serious threat to the safety of people and property, involves the uncontrolled burning of fuel. In the period 2011-2013. according to the data of the Emergency Situations Sector, a total of 79.886 fires occurred in Serbia, in which 1.280 people were killed or injured. In 2012. fire damage in Serbia amounted to approximately fifty million euros (Cvetkovic 2020).

Forest fires are an increasingly common phenomenon in Serbia during the last fifteen years, and the years 2007. when more than 500 forest fires were recorded, and 2012. with more than 700 fires, stand out in particular (Cvetkovic 2020). Forest fires are the most devastating form of destruction of forest ecosystems in Serbia. On that occasion, large forest areas are destroyed in a short time, ecosystems are damaged and the habitats of many plant and animal species are damaged or destroyed.

Coniferous and mixed forests suffer the greatest damage from fires. All types of forests are not equally threatened by fire and, for example, coniferous forests are more endangered than deciduous forests, and certain types of trees are more sensitive than others. According to the degree of danger from fire, forests are classified into the following six categories: I degree - pine and larch forests; II degree - forests of spruce, fir and other conifers; III degree - mixed coniferous and deciduous forests; IV degree - oak and hornbeam forests; V degree - forests of beech and other deciduous trees; VI degree - thickets and non-vegetated areas (Cvetkovic 2020).

In general, there are three types of forest fires: a) underground, b) ground or surface c) high or canopy fire (Cvetkovic 2020). Underground fires in forests in Serbia are quite rare considering the type of forests and surface deposits. It is characteristic for them that the fire smolders under

the surface of the earth, when deposits of moss, peat, leaves, veins, etc. burn in the deeper layers. They usually occur at a depth of approximately 20 cm, bearing in mind that this is the depth of the mentioned layers. Ground fires are the most common in Serbia and mainly involve different combustible materials in the ground layers of forests - dry grass, bushes, litter and wood waste, because they contain an abundance of small, easily flammable particles. If certain conditions are met (a sufficient amount of combustible material), it often happens that ground fires easily reach the treetops and grow into high fires. The next type of forest fires are high fires, i.e. fires that engulf the tops of trees. The rapid action of the wind creates large tongues of flame, which can spread quickly with the help of fire vortex and an abundance of flammable sparks.

Lightning strikes are one of the most common causes of forest fires. When we talk about human activity as the cause of forest fires, we mean different types of explosions, inattention and gross negligence, as well as fires caused by intentional ignition.

4. CONSEQUENCES OF NATURAL DISASTERS IN THE TERRITORY OF THE REPUBLIC OF SERBIA

As stated in the introductory part of this paper, the consequences of natural disasters that occurred on the territory of Serbia are great. In addition to losses in material and cultural assets, the biggest tragedy and loss for Serbia is the lost human lives. By analyzing the available data, the conclusion is reached that the financial losses of natural disasters were huge. The floods in Obrenovac in May 2014. alone cost Serbia around 1.5 billion euros, which represents a big blow to its budget and caused decreased investments in certain projects. The biggest consequences were caused by devastating earthquakes, floods and forest fires.

4.1. Consequences of the earthquake

How serious an earthquake is a threat to the safety of the citizens of Serbia is evidenced by the fact that just one strong earthquake can kill hundreds of thousands of people, cause material damage of one billion dollars in less than a minute, interrupt tens of thousands of business operations and leave hundreds of thousands of people without a roof, job, etc. elementary conditions for life (Cvetkovic 2020).

The largest earthquakes, where in addition to material damage there were also losses of human life, hit Lazarevac in 1922. when an earthquake with an intensity of 6.1 on the Richter scale was recorded (Cvetkovic 2020). In 1927. Gornji Milanovac was hit by an earthquake measuring 5.9 on the Richter scale, where 7 people lost their lives (Assessment of Disaster Risk in the Republic of Serbia 2017). In 2010. an earthquake with an intensity of 5.4 on the Richter scale occurred near Kraljevo, when approximately 258 earthquakes with magnitudes from 1.0 to 4.4 on the Richter scale were registered over several days. Unfortunately, two people died, many were injured, while the value of the material damage caused was estimated at more than 100 million euros (Cvetkovic 2020). The damage to infrastructure facilities was extensive, and some residential facilities had to be demolished due to the unprofitability of reconstruction.

4.2. Consequences of floods

Based on the analysis of the available data, the conclusion is reached that the floods in the territory of Serbia, which in the past mainly occurred as a result of "water spilling from the riverbeds, along sections where there are no flood protection facilities built, as well as due to overflowing and demolition of protective facilities" (Assessment of the risk of disasters in the Republic of Serbia 2017). Significant and serious floods in the geospace of Serbia were recorded in 1999., 2000., 2005., 2006., 2007., 2009. and 2014. The locations where the biggest

floods occurred in the last two decades are: Obrenovac (2006., 2010., and 2014), Novi Pazar (2011.), Ljubovija, Aleksandrovac, Sabac, Aleksinac, Krusevac, Trgoviste, Bogatic, Mali Zvornik, Loznica (2010.), Valjevo, Babusnica, Pirot (2007.), PoZarevac, Kraljevo, Belgrade - Savski venac, Ub, Smederevo, Golubac, Indjija, Zemun, Surcin (2006.) (Disaster Risk Assessment in the Republic of Serbia 2017 .).

During July 1999. large torrential floods in the basins of the largest tributaries of the Velika Morava caused serious damage in Sumadija. On that occasion, numerous residential and commercial buildings were damaged and 30 bridges in the basins of Zapadna Morava, Jasenica, Kubrsnica and Lepenica were taken away. In 2000. the sudden melting of snow and heavy rainfall in the area of the Tisa and Tamish watercourses caused serious floods. Intense rains in May 2014. in the territory of Serbia, northern Bosnia and eastern Croatia, caused serious flooding. According to their characteristics (territorial representation, duration, consequences, etc.), those flood events surpassed all previous ones (Cvetkovic 2020).

The characteristics of floods in Serbia are that arable land was completely or partially flooded, and agricultural crops were mostly destroyed in the areas affected by the floods. Infrastructure of various purposes, including parts of critical infrastructure, were partially damaged or threatened. The residential infrastructure near the flooded rivers was damaged, and the return of people to their homes was only possible after a couple of weeks, after drying and disinfecting the buildings. Due to sudden torrential flows on small rivers and streams, which caused landslides, many village roads were damaged and some places were cut off. The material damage was measured in millions of euros, up to 1.5 billion, which is the amount of the flood damage in Obrenovac in 2014.

4.3. Consequences of forest fires

Large forest fires affect Serbia every ten years. The last big fires hit Tara and the immediate surroundings of Cacak in August 2012. when about 10.000 hectares of forest were damaged (Nedeljnik Vreme 2012). Underground fires have the greatest consequences for forest ecosystems, because the product of fires is only smoke, which is difficult to see if it appears in areas far from settlements. On that occasion, the root of the plant is destroyed and such trees are condemned to death. The most frequent forest fires in Serbia are ground fires, which damage saplings and undergrowth as well as tree roots. High fires, as the rarest type of forest fires, are characteristic of young conifer and oak forests (Cvetkovic 2020). The fires in 2012. were a combination of all three types of fires that can occur in forest ecosystems. Because of this, a large forest area was destroyed, and extinguishing was extremely difficult due to the inaccessible terrain, and without help from the air it was impossible to bring the fire element under control. On that occasion, a large number of animal habitats were damaged or destroyed.

5. CONCLUSION

Natural phenomena, which often, due to the consequences for people's lives, material and cultural goods, took on the character of natural disasters, in the previous 100 years caused great suffering to Serbia and its inhabitants. Natural disasters have particularly intensified in the last twenty years, and the consequences are more devastating than before. Earthquakes, forest fires and floods have claimed a large number of human lives since the beginning of the 21st century, and the total financial losses are measured from hundreds of thousands, across millions and even all the way to billions of euros. A greater number of natural disasters than before are the result of climate change, which is directly related to the development and progress of industry, because unwanted products of industry affect changes in climate and natural ecosystems.

Increased population density and the development of cities located in large river basins have led to more lives lost in floods. Inadequate arrangement of the banks of large rivers and the

characteristics of the relief and riverbeds result in large river overflows during heavy rainfall. Heavy rainfall is the most common cause of floods, which claimed human lives and caused great material losses. The high population density of cities has also led to an increase in human losses in devastating earthquakes. Based on the data, it can be seen that the biggest consequences of the devastating earthquakes that hit Serbia were felt by the cities. Lazarevac, Gornji Milanovac, Kraljevo, the cities that felt the most diverse earthquakes in Serbia, in addition to great material losses, also lost many human lives as a result of the earthquake. The natural disaster that affects Serbia every ten years, in the majority of cases, did not claim human lives, but it left great consequences.

REFERENCES

Mladjan D. (2015). Bezbednost u vanrednim situacijama. Kriminalisticko – policijska akademija, JP „SluZbeni glasnik“, ISBN 978-86-7020-309-9, Beograd.

Cvetkovic V., (2020.), Upravljanje rizicima u vanrednim situacijama, Naucno – strucno drustvo za upravljanje rizicima i vanrednim situacijama, Neven DOO, ISBN 978-86-81424-02-5, Beograd.

Cvetkovic V., (2022.), Taktika zastite i spasavanja u katastrofama, Naucno – strucno drustvo za upravljanje rizicima i vanrednim situacijama, Neven DOO, ISBN 978-86-81424-09-4, Beograd.

Zakon i smanjenju rizika od katastrofa i upravljanju vanrednim situacijama. SluZbeni glasnik RS, br. 87/2018. Beograd.

Zakon o vanrednim situacijama. SluZbeni glasnik RS, br. 111/2009, 92/2011 i 93/2012.

MUP (2017.), Procena rizika od katastrofa u Republici Srbiji, Beograd.

<https://www.vreme.com/vreme/srbija-u-plamenu/>, Accessed: 01.09.2023.

<https://vokabular.net/litosfera/>, Accessed: 01.09.2023.

<https://vokabular.net/hidrosfera/>, Accessed: 01.09.2023.

<https://vokabular.net/atmosfera/>, Accessed: 01.09.2023.

<https://vokabular.net/biosfera/>, Accessed: 01.09.2023.

STRATEGIC DIMENSIONING OF THE DEFENSE SYSTEM OF THE REPUBLIC OF SERBIA BASED ON THE PHYSIOLOGY OF MODERN ARMED CONFLICTS

Katarina Jankovic^{1a}, Srecko Vukovic², Slavica Dabizljevic³

¹ General Staff of the Serbian Armed Forces, Directorate for Development and Equipping J-5, Technical Test Center, Center for Testing Weapons and Military Equipment, Nikinci, Republic of Serbia, jankovickatarina95@gmail.com

² General Staff of the Serbian Armed Forces, Directorate for Development and Equipping J-5, Technical Test Center, Center for Testing Weapons and Military Equipment, Nikinci, Republic of Serbia, srecko.vukovic99@gmail.com

³ RASEC, Belgrade, Republic of Serbia, cacabezbfc@yahoo.com

Received: 14th September 2023

Accepted: 18th September 2023

Professional paper

Abstract: *Armed conflict as a social phenomenon is an often studied topic, but its research is always a challenge, especially since it is a changing social phenomenon that evolves in time and space, with all its peculiarities, carrying a part of its unchanging character. For all those who in any way participate in the formulation of the defense strategy, it is extremely important to first accept that there have been changes in the physiognomy of modern armed conflicts and that, for the sake of its understanding, strategic, conceptual, critical and systemic reflection is imposed as necessary access. The defense system represents the overall organization, equipment and capability of the state, its citizens, the army and other subjects of society (defense force) for the defense of its sovereignty, territory, independence and constitutional order. In this regard, the paper points out that modern armed conflicts, bearing in mind that they have always been the most serious form of threat to security, determine the way of dimensioning the defense system of the Republic of Serbia.*

Key words: *defense system, Republic of Serbia, armed conflict, national security*

1. INTRODUCTION

In the modern world, the defense system of a country plays a key role in preserving its security and sovereignty. However, nowadays, modern forms of armed conflicts impose the need for a new approach to the strategic dimensioning of the defense system. In this sense, this paper deals with the strategic dimensioning of the defense system of the Republic of Serbia, based on the study of the physiognomy of modern armed conflicts.

The Republic of Serbia as a country went through turbulent times during the 20th century, including two world wars, wars in the former Yugoslavia and NATO bombing. All this has

^a ORCID: 0009-0006-0988-4895

influenced the development of the defense system of the Republic of Serbia, which today faces numerous challenges, risks and threats, including terrorism, cyber attacks, organized crime and instability in the region.

The development of the defense system of the Republic of Serbia must be harmonized with modern trends in armed conflicts, which are increasingly complex and dynamic. This paper aims to contribute to the understanding of modern security threats and their impact on the strategic dimensioning of a defense system that is capable of overcoming them.

2. PHYSIOLOGY OF ARMED CONFLICTS

The physiognomy of armed conflict deals with the study of various aspects of conflict, including military tactics, strategy, psychology, geopolitical frameworks, and social conditions that influence conflict. Modern armed conflicts are characterized by the speed of development, the mobility of forces, the scope and range of targets and the use of sophisticated techniques. Consequently, the actors and participants in the conflict have evolved. Therefore, it is necessary that the strategy and approach to the defense of the Republic of Serbia adapt to these changes and be based on the analysis and understanding of the physiognomy of modern armed conflicts, which is dealt with in the rest of the paper. The specificity of modern armed conflicts requires new approaches to observation and analysis of causes and consequences. Namely, the perpetrators of armed conflicts are not only military forces, but the character of the conflict includes all factors in the territory it covers. In addition to military forces, the civilian population, economy, social stability, critical infrastructure, etc. are also important factors.

2.1. The evolution of the physiognomy of armed conflicts

It should be emphasized that armed conflicts, and with them the army and weapons, have been constant companions of the development of human society since the emergence of organized socio-economic communities (societies). This was the case in all previous socio-economic formations: slavery, feudalism, capitalism, and even failed socialism, with each new conflict being greater than the previous one both in terms of intensity and scale.

German General Franz Uhle-Wettler wrote: "Earlier, the commander could be sure that the future war would be similar to past and current wars. This allowed him to analyze appropriate tactics from the past and present. The one who commands the army today no longer has that possibility. He only knows that whoever fails to learn from the past war will surely lose the next one." (Williams et al., 1989).

In modern armed conflicts, with the development of technology, the physiognomy of the conflict has changed even more. Today, armed combat is mostly conducted from a long distance, with the use of drones and autonomous weapons, which significantly reduces physical contact between opposing forces. Also, modern technology enables better tactical planning and coordination of participants in armed combat, which leads to more precise and efficient execution of tasks.

2.2. New actors and participants in armed conflicts

In the last few decades, the world has witnessed the emergence of new actors and participants in armed conflicts. Based on the analysis of the literature in which different actors and participants in armed conflicts were analyzed, the conclusion can be drawn that traditional state actors, such as the army and the police, have faced new enemies such as terrorist groups, paramilitary organizations, private military companies, criminal networks, non-governmental organizations, hacker groups, etc. These new actors differ from traditional state forces in terms of structure, motivation and mode of action, as they do not rely on state resources and authority, but act in accordance with their own goals and interests.

Terrorist groups represent a global security challenge because, through a violent form of political activism, they threaten the security of the state and its citizens. Their goal is to achieve changes in society, the state or the world through political or ideological means. Terrorist groups are small, mobile and operate in secret. They often use guerilla warfare tactics, such as surprise attacks, sabotage and assassinations.

Paramilitary formations are organized military or police units that work outside the framework of regular institutions. They are usually formed by individuals or groups who want to achieve their goals that do not comply with laws and regulations. Paramilitary formations often use violence as a means to achieve their goals and are often associated with organized crime. They are also prone to violating international humanitarian law, such as rules on the protection of civilians and prisoners of war.

Private military companies are a relatively new phenomenon in armed conflict and are usually contracted to provide security and military services to the government or other organizations. However, they are often criticized for their lack of transparency and oversight, which can lead to abuse of their powers and human rights violations.

Criminal networks have also become a significant actor in armed conflicts, especially in countries with weak institutions and high crime rates. They use various forms of violence, including kidnapping, blackmail, drug and human trafficking, and other illegal activities. These networks are capable of creating a major impact on society and the economy and represent a serious security challenge for states and international organizations. They are often connected with political and economic interests, as well as with terrorist and paramilitary groups. Criminal networks are often used as a source of financing for other actors in armed conflicts.

Non-governmental organizations (NGOs) are established outside the state and political structures to deal with social, humanitarian and political issues. Non-governmental organizations play an important role in providing assistance to victims of armed conflicts and implementing peaceful solutions to conflicts. Their work can be threatened by violence and instability in the countries where they operate. However, some NGOs have been criticized for political or ideological biases^b.

Hacker groups can be said to be new entrants to armed conflicts in the sense that they use cyber-attacks to influence world events. These groups may have politically or ideologically motivated goals, as well as the goals of violating privacy, stealing financial resources, and threatening the security of companies or countries. Hacker groups have proven to be "powerful" players in the cyber security world and can cause significant damage. In addition, they can influence elections and political processes, providing support to one or the other side

^b Examples of some non-governmental organizations that have been criticized in modern armed conflicts:

- Human Rights Watch - an organization that deals with the protection of human rights in the world, but was criticized for its political bias in the case of Syria and Palestine, as well as for its non-objectivity in portraying some events.
- Médecins Sans Frontières - an organization that deals with medical aid to countries at war, but has been criticized for political bias in the case of Syria and Palestine.
- World Peace Council (World Peace Council) - an organization that advocates for the peace process in the world, but was criticized for its ideological bias in the case of Syria and Yemen. These criticisms are not necessarily entirely accurate, and each organization is entitled to its own opinions and views. However, it is important that non-governmental organizations are open to dialogue and work to protect the interests of the wider community.

in conflicts. However, it is important to note that hacking is illegal and cyber security breaches are punishable by law. Therefore, investing in cyber security and training personnel in this area is considered important and necessary, in order to defend against potential cyber attacks.

The above indicates that the emergence of new actors and participants in armed conflicts represents a challenge for traditional state forces and the international legal framework that regulates this area. In order to respond to these new threats, it is necessary to adapt the approach to the defense of the state. It is necessary to recognize the differences in their structures, motivation and methods of action, as well as to find new ways of fighting against them while simultaneously respecting international humanitarian law and human rights.

2.3. Basic characteristics of modern armed conflicts

The wars that were fought or are being fought after the breakup of the Eastern Bloc are called by most analysts the wars of the modern era (Delibasic et al., 2017). It is very difficult to apply the classic Clausewitzian approach to modern armed conflicts, which implies that war begins with the declaration of war, and that it is based on cruel but legitimate actions.

Modern armed conflicts are more and more complex and often differ from the classical conflicts in wars as we knew them in the past. The causes of armed conflicts are complex and diverse, and the actors participating in them are increasingly diverse. Precisely because of this, modern conflicts are characterized by some basic characteristics that make them unique. Based on the analysis of the literature dealing with various aspects of contemporary armed conflicts, the following common features can be drawn:

1. Asymmetry: Modern armed conflicts often involve an imbalance of power between opposing parties. Generally, one side is better equipped, trained and has more resources than the other side. This can lead to various forms of armed conflict, such as guerilla warfare, terrorism and other forms.

2. Continuity: Modern armed conflicts do not exist in the form of formally declared wars, but take place through a series of minor incidents, terrorist attacks and other forms of violence. This can lead to a big difference between the conditions of peace and war and affect the stability of society and the state. A frequent phenomenon in the modern world is that there is no clear boundary between the state of war and peace (Kovac and Stojkovic, 2009).

4. Interdependence and cooperation of interspecies forces: Modern armed conflicts within the framework of modern operations will be conducted primarily as joint interspecies operations. Since the danger of weapons of mass destruction has increased significantly, the armies are required to be trained to successfully carry out combat operations in the conditions of the use of nuclear, chemical and biological warfare agents (Kovac and Stojkovic, 2009).

5. Use of new technologies: Modern armed conflicts include the use of new technologies, such as drones, autonomous weapons, biological and chemical weapons, etc. This can affect the way armed conflict is conducted, as well as the possibility of protecting civilians in combat zones. The development of modern means, tools and weapons enables, at the same time, the successful conduct of combat operations on land, sea, airspace, underwater and outer space (Kovac and Stojkovic, 2009).

6. Connectivity: Contemporary armed conflicts involve an international network of participants, state and non-state actors. This can lead to the spread of conflict, making it difficult to establish peace.

7. Impact on the civilian population: Contemporary armed conflicts affect the civilian population in a variety of ways, including forced displacement, injury, destruction of

infrastructure and economic destruction. This is why the protection of civilians has become an important aspect of modern armed conflicts.

8. Struggle for dominance over the adversary on the IT front: It is important to timely collect accurate information that is delivered to commanders at all levels in order to make adequate decisions, but on the other hand, to prevent the successful activities of the enemy on that front.

9. Contemporary armed conflicts are often not isolated but part of contemporary crises: Contemporary armed conflicts are often not isolated and independent events, but are part of a wider crisis context that may include economic, political, social and cultural dimensions. For example, a conflict in a state may be the result of a political crisis that has resulted in social unrest and rebellions against the government. These conflicts can also have a regional or international impact, making them part of a wider global context. Contemporary armed conflicts that are part of a wider context can have serious consequences for the security and stability of states and regions. They can lead to humanitarian disasters, loss of life and property, population displacement, radicalization, strengthening of extremist movements and terrorism.

Analyzing the mentioned characteristics of modern armed conflicts, one gets the impression that they are becoming more and more difficult to find a solution. Therefore, it is necessary to invest more efforts in understanding these characteristics and to look for new and innovative ways to overcome modern armed conflicts, especially through strengthening international cooperation, protecting the civilian population and preventing the escalation of conflicts to a new level of violence. Understanding the basic features of modern armed conflicts is also key to creating a more stable and secure environment.

3. DEFENSE SYSTEM OF THE REPUBLIC OF SERBIA

Article 51 of the United Nations Charter defines that the right to defense is one of the basic principles of the national security policy, which is based on the basic rights and sovereignty of the state. This right provides every member of the United Nations to defend themselves in the event of an armed attack. Consequently, Serbia, as a member of the United Nations, has the right to defend itself in the event of an armed attack. The defense interests of the Republic of Serbia are realized through the defense policy, which is one of the elements of the national security policy

The defense system of the Republic of Serbia is part of the national security system and represents a unique, structurally organized and functional unit of defense forces and entities whose goal is to protect the defense interests of the Republic of Serbia (Kovac, 2009). Protection of defense interests is a unique function of the state and is realized through military and civil defense. The bearer of military defense is the Serbian Army, and in the implementation of civil defense, state bodies, state administration bodies, bodies of autonomous provinces, bodies of local self-government units, business companies, public services and other subjects and forces of the defense system are involved.

In Serbia, the first National Security Strategy (NSB) was adopted in 2009^c. This part of the document, by title, is identical in both strategies. The main difference between the new document (2019) and the previous one (2009) is: 1) challenges, risks and threats are more correctly systematized and named compared to the 2009 document; 2) certain challenges, risks and threats are stated differently; 3) formally, the number of identified challenges, risks and

^c Before that, the documents that defined the challenges, risks and threats to security were: The White Book of Defense of the State Union of Serbia and Montenegro from 2005 and the Strategic Review of Defense from 2006.

threats is smaller in the new document (2009 National Security Strategy and 2019 National Security Strategy).

The mentioned challenges, risks and threats are not only a problem of the Republic of Serbia, but also of the entire region and the world. That is why it is important that the state and the authorities of the defense system accept these facts and take measures to improve the security of all citizens and protect the state from external and internal threats. Such an approach requires long-term and systematic planning, cooperation with other countries and international organizations. Finally, with good planning, cooperation and investment in security, the defense system of the Republic of Serbia can provide a safe environment for all its citizens.

The defense system is based on the existing Constitution of the Republic of Serbia^d, its laws and international agreements and conventions ratified by the Serbian Parliament. The defense of the Republic of Serbia is realized by the engagement of available human and material resources, and is ensured by the use of the Serbian Armed Forces and other defense forces to protect sovereignty, independence, territorial integrity and security (Law on Defense, Belgrade, 2007).

The structure of the defense system, as a part of the national security system, consists of the bodies of the legislative and executive authorities of the Republic of Serbia, the Serbian Armed Forces, civil defense and other entities important for defense. The bodies of the legislative and executive authorities of the Republic of Serbia, within their regular competences and responsibilities prescribed by the Constitution and the law, manage the defense system and ensure the conditions for the stable functioning of the defense system of the Republic of Serbia, both in peace and in times of war and emergency. The Serbian Army defends the country from armed threats from the outside and performs other missions and tasks in accordance with the Constitution, the law and the principles of international law that regulate the use of force (Defense Strategy of the Republic of Serbia, 2019). Civil defense is part of the unified defense system. It is organized at the level of the Republic of Serbia, autonomous provinces and local self-government units (Defense Strategy of the Republic of Serbia, 2019). Other subjects important for the defense of the Republic of Serbia are institutions that deal with affairs in the fields of diplomacy, security, economy, education, health, science and information, as well as legal entities whose activities contribute to the functioning of the defense system. Holders of jobs and activities of importance for defense perform tasks in coordination with entities of the defense system, in accordance with the law (Defense Strategy of the Republic of Serbia, 2019).

The structure of the defense system of the Republic of Serbia is complex and includes subjects, forces and institutions in the country. The structure of the defense system is aligned with the defense strategy of the Republic of Serbia and aims to defend the country against various threats to national security. This implies the immediate defense of the territory, participation in international peacekeeping missions, all with the aim of ensuring peace and stability in the region and the world.

^d In addition to the Constitution, the defense system of the Republic of Serbia is governed by the following laws: Constitutional Law for the Implementation of the Constitution of R. Serbia; by the Law on the National Assembly; by the Law on the President of the Republic; Law on Government; by the Law on Ministries; Law on Defense; the Law on the Serbian Armed Forces; Law on the use of the Serbian Armed Forces and other defense forces in multinational operations outside the borders of the Republic of Serbia; Law on Military Security and Military Intelligence Agency; The Law on Military, Labor and Material Obligation, and the Law on Civil Service

4. DESIRED CHARACTERISTICS OF THE DEFENSE SYSTEM OF THE REPUBLIC OF SERBIA DEVELOPED ON THE BASE OF THE STUDY OF MODERN ARMED CONFLICTS

The defense system of the Republic of Serbia aims to protect the territory and the population, as well as to contribute to peace and stability in the region and the world. In this sense, it is necessary for the defense system to be developed in accordance with the requirements of modern armed conflicts and to have appropriate characteristics that will make it efficient and reliable. In this paper, some of the most important characteristics of the defense system of the Republic of Serbia are discussed, namely: permanence, adaptability, ability to update, transparency and specificity. These characteristics were developed based on the study of modern armed conflicts and aim to prepare the defense system of the Republic of Serbia for the challenges that await it in the future.

Continuity – the defense planning process is continuous, planning cycles are repeated, plans are extended and updated. Permanence is one of the desirable characteristics of the defense system of the Republic of Serbia, which implies that the defense system should be able to function in the long term, to meet the needs and conditions of future generations, and to be able to adapt to changes in state policy and global changes. This means that the defense system must be reliable and continuously functional. In modern armed conflicts, the speed of reaction and the efficiency of the defense system are key factors for achieving success. The permanence of the defense system means that there must be constant concern for the maintenance of the system, its modernization and improvement in order to maintain the ability to act in the conditions dictated by modern armed conflicts. The permanence of the defense system implies regular training and equipping of the forces of the defense system of the Republic of Serbia, which is of key importance for ensuring their readiness at all times.

The defense system of the Republic of Serbia should have a stable and sustainable financial model, have well-planned and pre-prepared reserves of material and technical assets and reserve units, have established plans for training and education of the forces of the defense system, and have high technological empowerment. A sustainable defense system also includes good cooperation with other states, institutions and organizations, in order to ensure peace and stability at the international level.

Adaptability - defense planning should have the ability to adapt to changes in the environment and ensure the constant transformation of the defense system. Adaptability is another important characteristic of the defense system of the Republic of Serbia, because new tactics and technologies are constantly being developed in modern armed conflicts. The defense system must be able to adapt to new challenges and adopt new technologies, so that it can effectively fight against modern security threats. The adaptability of the defense system of the Republic of Serbia implies the development of flexible and modular systems, which are easily adapted to changes in the environment, as well as the development of strategies that enable a quick response to unforeseen situations.

The adaptability of the defense system of the Republic of Serbia also implies quick decision-making in situations that require an immediate response, such as terrorist attacks or aggression by other countries. In such situations, the defense system of the Republic of Serbia must be flexible and capable of quickly adapting to new situations in order to ensure effective protection of citizens and territory.

In a world where technologies and strategies change rapidly, the ability to adapt is vital to effectively protect the state and citizens. For this reason, the defense system of the Republic

of Serbia must be constantly improved in order to remain adaptive and capable of dealing with all the challenges that may arise in modern armed conflicts.

Updateability – defense planning should ensure that plans are updated based on changes in the environment (threats, resources, priorities). This desirable feature of the defense system of the Republic of Serbia implies regular updating of the system, including IT equipment, as well as the policies and procedures used to manage the defense system. The defense system must be able to quickly adapt to changes in technology and tactics used in modern armed conflicts, as well as to changes in geopolitical circumstances. The ability to update a defense system can be crucial to maintaining its efficiency and effectiveness in the function of national defense.

Transparency - Transparency refers to openness in the operation of the defense system, including decision-making, costs, equipment procurement, resource management, etc. The Republic of Serbia strives to ensure transparency in its defense policy in order to enable greater efficiency and effectiveness, but also to gain the trust and support of the public.

It is often complained that the defense system of the Republic of Serbia is not transparent enough, especially when it comes to costs and the procurement of equipment. It is precisely for this reason that transparency is one of the key desirable characteristics that develop on the basis of modern armed conflicts. Transparency in the operation of the defense system also helps prevent corruption and misuse of resources, which is vital for protecting national security.

Propaganda and disinformation are often used in modern armed conflicts, so it is important for the defense system to be transparent in order to provide accurate information about the situation on the ground. This will help fight misinformation and manipulation and ensure that the public has a clear and true picture of the events that are taking place.

A high level of transparency in the defense system can improve cooperation with other countries, which is of great importance in international relations. This may include the sharing of information on military exercises and operations, the joint planning and execution of operations, and the sharing of expertise and technology.

Specificity - each country should have a specific defense planning system that is harmonized and interoperable with defense planning in international organizations (eg with defense planning in NATO or the EU). Specificity can also refer to the ability of the defense system of the Republic of Serbia to adapt to the specific challenges and threats it faces. In the modern world, armed conflicts are very diverse and can be of different nature, from terrorism to hybrid wars, cyber attacks and other new forms of aggression.

The specificity of the defense system of the Republic of Serbia may also be the need to respond to the specific geographical conditions and circumstances of modern armed conflicts. The territory of the Republic of Serbia includes mountains, forests, rivers and lakes, and it is also located in an unstable region. To respond to these specific circumstances, it is necessary for the defense system to be able to adapt to different terrain conditions and to use different tactics and strategies that are effective in different environments.

Due to all of the above, it is necessary to adapt the defense system of the Republic of Serbia to new and specific forms of armed conflict that occur in the modern world. This capability is achieved through the development of new strategies, tactics and technologies. It is also important to carry out continuous education and training of subjects and forces of the defense system in order to adequately respond to new forms of modern armed conflicts. The specificity of the defense system is crucial for ensuring an effective and efficient defense of national security.

The research of modern armed conflicts provides important guidelines for the strategic development of the defense system of the Republic of Serbia. The fact that armed conflicts are continuously changing and developing emphasizes the importance of constant improvement of the defense system, as well as the need to develop the ability to adapt to new circumstances. It is important that the defense system be transparent and enable citizens to participate in the decision-making process, while at the same time being specific and adapted to the needs of the Republic of Serbia. Taking into account the above characteristics, it is possible to develop an effective defense system that will ensure the protection of the state and its citizens in the modern world.

5. CONCLUSION

The strategic dimensioning of the defense system of the Republic of Serbia based on the study of modern armed conflicts is essential for the preservation of national security. The evolution of the physiognomy of armed conflicts and the appearance of new actors and participants represent a challenge for every country, including the Republic of Serbia. Therefore, the defense system must be adaptive and able to be updated, with transparent and specific characteristics. The management of the defense system must be in accordance with the principles of functionality and efficiency. Only such a system will be able to ensure the safety of citizens and the state in modern armed conflicts.

Conflicts in the surroundings of the Republic of Serbia are a current threat, with no prospect of ending in the future. The quantity and immediacy of this threat are the subject of future research and analysis, but they certainly have a significant place in the dimensioning and development of the defense system of the Republic of Serbia. The elaboration of the characteristics of the defense system in this paper shows that the defense system must not only be a representative of the physical force with which it should guarantee its sovereignty and territorial integrity. The physiognomy of modern armed conflicts points to a broader spectrum of challenges, risks and threats that have an impact on the security of the Republic of Serbia. In this light, it is necessary to research and determine the characteristics of the defense system, based on which it is possible to dimension the defense system, with capabilities that enable adaptability to all challenges, risks and threats.

Contemporary armed conflicts and their characteristics are of essential importance for the dimensioning of the defense system of the Republic of Serbia. Given that the Serbian Army is a pillar of the development of the ability to conduct armed conflicts, the ability to deter aggression based on its equipment with modern combat systems and an organization that enables the performance of set tasks is given a special dimension. The essential element of the aforementioned capability is the development of the necessary defense resources, when the internal element is concerned, that is, the development of alliances and the support of friendly states, when the external element is concerned.

A significant feature of modern armed conflicts is the multidimensionality of the consequences for the civilian population and critical infrastructure. Although, by definition, military force should act according to military objectives, modern conflicts show that more than military units and resources, civilian soldiers, cultural heritage and the environment suffer. This is proof that armed conflicts are no longer isolated, in terms of time, space and consequences, but that they are part of a wider picture of crises in a certain area. As crises do not have defined frameworks, armed conflicts, of which they are a part, have undefined frameworks, ways and goals of action. Although the actors try to show that their goal is to act on military goals, the fact is that with one military goal, a greater number of elements of civil society suffer. The above indicates that the modern defense system of the Republic of Serbia must be based on a multidimensional analysis of challenges, risks and threats observed in the light of modern

crises, in order to analyze all aspects of the consequences of armed conflict and ensure adequate development of the capabilities of the defense system.

REFERENCES

- Delibasic D., Talijan M., Jevtic D. (2017) Fizionomija savremenih oruzanih sukoba kroz prizmu oruzanog sukoba u Ukrajini, Vojno delo, broj 1
Zakon o odbrani, Beograd, Sluzbeni glasnik 116, 2007.
- Kovac, M., Stojkovic, D. (2009), Strategijsko planiranje odbrane, VIZ, Beograd
- Kovac, M. (2009), Politicka i vojna neutralnost Republike Srbije. U M. HadZic, i J. Radoman, Ekonomija i bezbednost . Beograd: Centar za civilno-vojne odnose.
- Kovac, M., Stojkovic, D., i Mitic, V. (2013), Capability based defence development planning- Optimal option selection for capability development. XI Balkan Conference on Operational Research- BALCOR 2013. Beograd: Fakultet organizacionih nauka. 36)
- Kovac, M., Stojkovic, D., i Mitic, V. (2014): The model of organizational capabilities development. SYMORG. Beograd: Fakultet organizacionih nauka.
- Mackic, R. (2013), Strategijski koncept odbrane Republike Srbije. Vojno delo
- Mihailovic, T. (2020), Upravljanje sistemom odbrane Republike Srbije, Fakultet bezbednosti
- Mitic, V., Kovac, M., i Kankaras, M. (2017), Model procene strategijskog okruzenja sistema odbrane. Vojno delo, 2017.
- Strategija nacionalne bezbednosti Republike Srbije, Sluzbeni glasnik Republike Srbije, br. 88/09.. 2009
- Strategija nacionalne bezbednosti Republike Srbije, „Sluzbeni glasnik RS“, broj 94, 2019
- Forca, B., Sekulovic, D. (2017): Identifikacija problema savremenih strategija bezbednosti: studija slucaja – Republika Srbija, Zbornik radova sa nacionalnog naucnog skupa „Savremeni problemi strategije i strategijskog menadzmenta“, Fakultet za poslovne studije i pravo, Beograd
- WilliamS. Lind, Keith Nightengale, John F. Schmitt, JosephW. Sutton, GaryI. Wilson, (1989) „Promenljivo lice rata ka cetvrtoj generaciji“, „TheChangingFaceofWar: IntotheFourthGeneration“, Marine Corps Gazette

CONFERENCE ORGANIZERS



RASEC
Regional association for security and crisis management

REGIONAL ASSOCIATION FOR SECURITY AND CRISIS MANAGEMENT



S4 GLOSEC GLOBAL SECURITY

COORGANIZERS



**FACULTY FOR SECURITY STUDIES
– EDUCONS**



**KARLOVAC UNIVERSITY OF
APPLIED SCIENCES**



**FACULTY OF OCCUPATIONAL
SAFETY UNIVERSITY OF NIS**



**COLLEGE OF BUSINESS AND
TECHNICAL EDUCATION,
DOBOJ, BOSNIA AND
HERZEGOVINA**



**RESEARCH CENTER
BANJALUKA**



FACULTY LOGISTICS CELJE

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

005.334(082)

351.78(082)

351.861(082)

INTERNATIONAL Scientific-Professional Conference - Security and Crisis Management - Theory and Practice SeCMan - International Forum "Safety for the Future" 2023 (9; 2023 ; Belgrade)

Proceedings / 9th International Scientific-Professional Conference - Security and Crisis Management - Theory and Practice SeCMan - 9th International Forum "Safety for the Future" 2023, September 29 and 30 Belgrade 2023 ; [editorial Nenad Komazec, Branko Babic]. - Belgrade : Regional Association for Security and Crisis Management: S4 GLOSEC Global security, 2023 (Beograd : Donat graf). - 376 str. : graf. prikazi ; 24 cm

Tiraž 75. - Bibliografija uz svaki rad.

ISBN 978-86-80692-10-4 (RASCМ)

а) Кризни менаџмент -- Зборници б) Ванредне ситуације -- Управљање -- Зборници
в) Безбедносни сектор -- Зборници

COBISS.SR-ID 125304073

