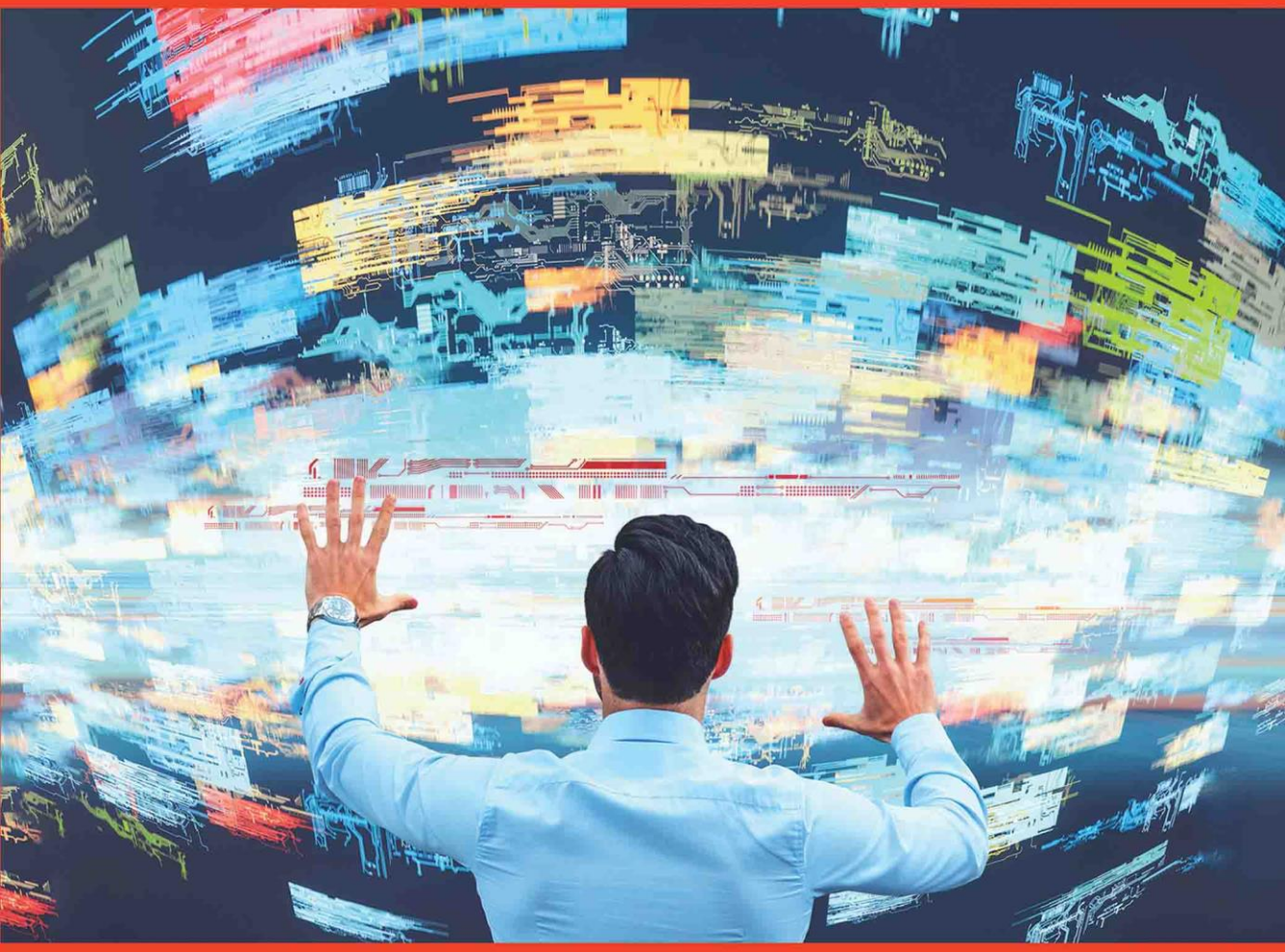


HOW TO DEAL WITH UNCERTAINTIES IN INCREASINGLY COMPLEX ENVIRONMENT? (THE NEW CARTOGRAPHY OF RISK AND CRISES)

PROCEEDINGS OF THE INTERNATIONAL SCIENTIFIC CONFERENCE HELD IN CAVTAT - DUBROVNIK SEPTEMBER 27-29, 2022

How to deal with uncertainties in increasingly complex environment?

(The new cartography of risk and crises)

Proceedings of the international

scientific conference held in Cavtat – Dubrovnik

September 27-29, 2022

PUBLISHERS:

Faculty of Philosophy – Institute for Security, Defense and Peace, "Ss. Cyril and Methodius" University

Center for Risk Analysis and Crisis Management (CARUK), Belgrade, Serbia

Institute for Standardization of Serbia (ISS)

Faculty of Criminal Investigation, Criminology and Security Studies, University of Sarajevo

EDITORS:

Prof. dr Zoran Keković, Faculty of Security Studies, University of Belgrade

Prof. dr Ratko Duev, Faculty of Philosophy, "Ss. Cyril and Methodius" University

Doc. dr Jadranka Polović, Croatian Association for International Studies, Zagreb

REVIEWERS:

- Prof. dr Robert Mikac, Faculty of Political Science, University of Zagreb, Croatia
- Prof. dr Elizabeta Ristanović, Military Medical Academy, Belgrade, Serbia
- Prof. dr Anni Dasho, Luarassi University, Tirana, Albania

EDITORIAL BOARD:

- Prof. dr Zoran Keković, Faculty of Security Studies, Belgrade, Serbia
- Prof. dr Oliver Bakreski, Faculty of Philosophy, "Ss. Cyril and Methodius" University
- Prof. dr Jasmin Ahić, Faculty of Criminal Investigation, Criminology and Security Studies, University of Sarajevo, B&H
- Milan Marković, Faculty of Political Sciences, University of Montenegro, Podgorica
- Prof. dr Mirsada Hukić, Academy of Science and Arts of B&H, European Academy of Science (EAS), Faculty of Medicine of the University in Tuzla, B&H
- Prof. dr Krešimir Pavelić, Faculty of Medicine, Pula, Croatia
- Prof. dr Želimir Kešetović, Faculty of Security Studies, Belgrade, Serbia
- Dr Marija Đorić, Institute for Political Studies, Serbia
- Ms Nevena Stanković, Youth Network for Strategic Risk and Crisis Management, Serbia

Translation and proofreading in English: Tanja Milošević

Technical Assistant: Ana Lalić

Printed by:

Copies:

C O N T E N T

Dear readers,

Nowadays, it is a known fact that modern risks are multifaceted and multidimensional. They are political, economic, security, technological, health, environmental, etc., and require a multi-centered perspective, given that they imply contemporary risks, when speaking of their prevention and control. Precisely because of the changing nature of the modern challenges, the synergy of natural, social and technical sciences is essential when speaking of reaching the goal of creating new knowledge and solutions in order to respond to complex challenges, and above all, strengthen the resilience of society and establish management mechanisms that recognize the new reality. This was confirmed by the *COVID-19* pandemic, which emerged as a health, but also geopolitical, security and economic challenge, but also by other tensions that constantly imprint a new dimension of mistrust and competition between the great powers in the field of international relations.

The previously defined thematic framework brought together some of the leading researchers, scientists and experts from the Western Balkans, who joined their forces at the international conference entitled "How to deal with uncertainties in an increasingly complex environment – New cartography of risks and crises", that was held in the hotel "Croatia" in Cavtat, on September 29-30.

The two-day conference justified the expectations of numerous participations from the academic society, public agencies and business community, as well as the organizers and partners, given that the lecturers were some of the most prominent regional and Western European experts in strategic risk and crisis management, originating from the following institutions: Center for Risk Analysis and Crisis Management (Belgrade), Croatian Association for International Studies (Zagreb), Faculty of Criminalistics, Criminology and Security Studies of the University of Sarajevo, Faculty of Philosophy (Institute for Security, Defense and Peace) of the University "Ss. Cyril and Methodius" in Skopje, and the Institute for Standardization of Serbia (ISS). The conference was conducted in partnership with the Institute for Strategic Risk Management (London), the Faculty of Political Sciences of the University of Montenegro, the "Luarasi" University from Tirana and the Youth Network for Strategic Risk and Crisis Management. Bearing in

mind the complex circumstances we are facing and the necessity to emphasize the academic and professional dialogue, lecturers from the region, thus including lecturers from Croatia, Serbia, Bosnia and Herzegovina, Montenegro, Albania and Macedonia, as well as Great Britain, Italy, Finland, Sweden, the Netherlands and Australia, presented the results of their research and offered functional recommendations for successfully overcoming the problems in question.

Opting for a multidisciplinary approach to contemporary security challenges, aware of the fact that a long-term solution must be sought for in linking different academic disciplines and through a multidisciplinary concept discussion, the authors of the texts of the proceedings: "How to deal with uncertainties in increasingly complex environment – New cartography of risk and crisis" recognized that the modern world is at a historical transition, in the conditions of contemporary crises and unprecedented new challenges. Changing the width of their perception through various multidisciplinary insights is imposed as an imperative in the process of discovering new knowledge and scientific truths, based on the need for new policies and approaches to management in the time that stands before us. All the more so, as the challenges, risks and threats that marked the beginning of the 21st century exposed all the weaknesses of the current policies and institutional mechanisms for dealing with them. Epidemics, migration, terrorism, climate change, CBRN threats, cyber-attacks, and many future challenges touched upon by the authors of the papers presented in these proceedings, include a wide range of insecurities that we face today, and they inevitably affect states, societies, organizations, but also individuals. They emphasize the global character of the modern security, and, at the same time, the importance of the growing interdependence of scientific disciplines in the process of shaping reality and future security practices.

The procedings that lay before you are consisted of three parts: Geopolitical and Security Challenges in the Light of COVID-19 and the Ukrainian Crisis, including the Environmental and Energy Challenges; Critical Infrastructure Protection; and International Standards on Security and Resilience with anemphasis on the issue of Pandemics and Epidemics.

In the first part of the Proceedings, the papers thematize extremism, migrations, war, environmental and energy challenges from a security, political, legal and philosophical perspective.

In the second part of the Proceedings, entitled "Critical Infrastructure Protection", the authors examine various approaches and methods in protecting national infrastructure systems in different contexts, with a special emphasis on the conditions of pandemics, CBRN threats and cyber threats.

The last part of the proceedings summarizes international standards and best practices in fostering organizational and community resilience, emphasizing experiences, scientific and critical attitudes stemming from pandemics and other security issues.

Having all the previously mentioned in mind, we can thus conclude that the contemporary risk and crises have once again reiterated the necessity of analyzing the lessons learned and constructing strategies based the acquired experiences, in order to ensure better outcomes of our future encounters with similar security challenges, which are deemed to happen often in the future.

At the very end, we offer our sincere gratitude to all the authors of the papers published in the Proceedings of "How to deal with uncertainties in an increasingly complex environment – New cartography of risks and crises", with high hopes that our joint efforts will provide a good insight and a strong basis for dealing with the uncertainties that await us in the future.

In Belgrade, March 2023. **In the name of the Editorial Board,**

Prof. dr Zoran Keković

PART ONE: GEOPOLITICAL AND SECURITY CHALLENGES + ENVIRONMENTAL AND ENERGY CHALLENGES

Marija Đorić*)

UDC: 316.647.7(497-15)

HOW TO DEAL WITH VIOLENT EXTREMISM IN THE WESTERN BALKANS?

Abstract: *Violent extremism represents one of the biggest contemporary global problems that did not miss the Western Balkans. The main goal of the author is to research the specificities, forms and drivers of violent extremism in the Western Balkans, based on which the adequate approach to prevention and combatting this violent extreme phenomenon will be depicted. The prevention of violent extremism is of essential significance, having in mind that, in this way, the occurrence of terrorism, which is an even more complex security problem, is prevented. With the use of the method of comparative analysis, the author will reach a conclusion regarding the similarities and differences among the Balkan states when speaking of the attitude towards violent extremism. Besides the analysis of strategic and institutional approaches, the focus will be set on actions of the international factors, as well as the academic community and the civil sector, who are in fact the unavoidable actors in this field. Through the analysis of different approaches in the Western Balkans, the author will attempt to discover weaknesses, but the good examples as well, in the context of facing violent extremism. The expected result is depicted in certain innovative approaches, put in the service of degrading violent extremism to a marginal occurrence.*

Key words: *extremism, violent extremism, Western Balkans, radicalization, terrorism, security.*

INTRODUCTION

Violent extremism is a global phenomenon faced by numerous countries world-wide, including the Western Balkans region. In the mere beginning, controversies surrounding the geographical term 'Western Balkans' should be put to the fore, given that, for a certain group of domestic theoreticians, the Western Balkans represents a political phenomenon of manipulative character.[1)] One of the most common explanations is that, in regional scientific geography, the Balkan peninsula is divided into East, North and South, as well as that Serbia could, geographically speaking, belong only to the Central Balkans, and by no means to the Western Balkans. However, the European bureaucracy started using this term informally in 1997, only to set it in official use by 1998, and thus, nowadays, this term is widely accepted and refers to the countries of former Yugoslavia (with the exception of Croatia and Slovenia), as well as Albania. At a second glance, the Western Balkans countries (Serbia, Montenegro, North Macedonia, Bosnia & Herzegovina, Albania) represent, at this moment, a region that is not quite a part of the EU, though it strives to become one.

[1)] See more in: Stepić, Milomir. 2012. „Zapadni Balkan: primer geografskog raspojmljivanja i geopolitičkog manipulisanja", *Nacionalni interes*, no. 3, pp. 9-34.

*) Senior Researcher at the Institute for Political Studies, Republic of Serbia.

Besides having a common foreign policy goal (depicted in the EU membership), the Western Balkans countries are linked by the not so glorious conflict past, which represent a new challenge in EU integration process. Still, if we focus on violent extremism, countries of the Western Balkans can learn a lot from each other, especially having in mind the fact that they are facing similar security issues and that, through joint regional approach, they could make wonders when speaking of prevention of extremism.

When speaking of the forms of extremism, the Western Balkans countries have, during the past decades, faced ethnic separatism and religious extremism, while in contemporary times, the region has witnessed an intensification and the rise of the extreme right-wing, as well as the extreme left-wing.

The goal of this research is to identify forms of violent extremism, and then, through strategic and institutional approach, present the method used by the countries of the Western Balkans in combatting this issue. Due to common past (as well as mutual language), the following countries of the former SFRY were selected as case studies: Serbia[2)], Montenegro, Bosnia and Herzegovina and North Macedonia.

1. VIOLENT EXTREMISM AS A PHENOMENON

Extremism falls to the specter of the most elusive social phenomena, given that it is conditioned by time, place of occurrence, as well as ideological motives. What one group of political actors sees as extremism, the other will deem as mutually accepted attitude or behavior. Thus, we cannot speak of a unique definition of extremism on a global level. One of the existing academic definitions stresses that extremism represents 'behavior and attitude that is borderline allowed, with a tendency of crossing that line' (Đorić 2014, 134-135). As a political (and above all, social) phenomenon, extremism can occur in different forms. One of the most common classification criteria in recent times is violence, based on which extremism is classified as violent or non-violent. Given that there is a thin line between these two forms of extremism, Schmid rightfully stressed that both forms of extremism represent "two sides of the same coin" (Schmid 2014, 15).

[2)] Without the autonomous region Kosovo and Metohija.

Violent extremism is a phenomenon that is increasingly being mentioned not only in national strategies, but international documents as well. On the international plan, OSCE represents an organization that coined the term PVERLT (Preventing violent extremism and radicalization that lead to terrorism), nowadays representing the vital part of OSCE antiterrorist activities. Even in 2012, this organization stressed in some of its documents (such as the Consolidated Framework in the Fight against Terrorism) that the fight against violent extremism is no longer solely a task of state institutions, but that the entire society should be involved (women, youth leaders, media, civil society, etc.).[3)] Still, the crucial moment in the institutional mapping of the phenomenon of violent extremism is believed to have taken place in 2015, when the administration of the president of the US Barack Obama officially declared the fight against violent extremism.[4)]

The United Nations as well are, to a great extent, dedicated to prevention of violent extremism and radicalization, and thus this organization organized a global meeting of the UNDP in Oslo in 2016, with a goal of preventing radicalization, all with the idea of preventing the spread of violent extremism.[5)] After this meeting emerged the UNDP conceptual framework for prevention of violent extremism, based on eight fundamental drivers of radicalization[6)], later adopted by OSCE as well.[7)] Passing of the UN resolution No. 2178 was very significant for the fight against violent extremism, given that it is based on prevention of radicalization and mobilization of individuals for participation in terrorist groups in foreign battlefields. The UN encouraged in their Action plan for prevention of violent extremism from 2015 all Member States to work on a comprehensive prevention of violent extremism through passing different strategies and action plans.

[3)] See more in: OSCE. December 7, 2012. DECISION No. 1063, OSCE CONSOLIDATED FRAMEWORK FOR THE FIGHT AGAINST TERRORISM. Accessed at: https://www.osce.org, 23.02.2019.

[4)] This fight was primarily directed towards groups with jihadi ideology, such as ISIS, Al Shabaab, etc. According to: Perry, Valery (ed.). 2019. *Extremism and violent extremism in Serbia: 21st-Century Manifestations of an Historical Challenge*, *ibidem*-Verlag, Stuttgart, p. 26.

[5)] See more at: UNDP. 2016. PREVENTING VIOLENT EXTREMISM THROUGH PROMOTING INCLUSIVE DEVELOPMENT, TOLERANCE AND RESPECT FOR DIVERSITY. Global Meeting, 14-16 March, 2016, Oslo. Accessed at: https://www.undp.org, 01.02.2022.

[6)] The following drivers are in question: 1. Impact of global politics; 2. Economic exclusion; 3. Political exclusion; 4. Inequality together with violation of human rights; 5. Dissatisfaction with the existent economic and social system; 6. Unacceptance of diversity in society; 7. Weak state capacities and lack of security; 8. Change of global culture (with a special emphasis on intensification of violence in the media).

[7)] See more in: OSCE. 2014. *Sprečavanje terorizma i borba protiv nasilnog ekstremizma i radikalizacije koja vodi ka terorizmu: Pristup putem rada policije u zajednici*, Vienna, p. 29.

Even though violent extremism has already entered the official documents on the international level, the issue of its definition is still of an amorphous character. Therefore, for example, for the USAID, violent extremism 'refers to advocating, engaging in, preparing, or otherwise supporting ideologically motivated or justified violence to further social, economic and political objectives'.[8)]

Regarding the UK's Crown Prosecution Service, violent extremism 'can be defined as the use of any means or medium to express views which foment, justify or glorify terrorist violence in furtherance of particular beliefs, behavior that seeks to provoke others to terrorist acts, foment other serious criminal activities, or fosters hatred which might lead to inter-community violence' (Wither 2016, 40).

With the goal of providing as much detailed explanation of violent extremism as possible, the OSCE established a term *radicalization that leads to terrorism and violent extremism*, which can be explained as a 'dynamic process whereby an individual comes to accept terrorist violence as a possible, perhaps even legitimate, course of action. This may eventually, but not necessarily, lead this person to advocate, act in support of, or engage in terrorism' (OSCE 2020, 7).

In the following chapters of this paper, the author will provide an analysis of institutional and strategic principles of four countries of the Western Balkans (Serbia, Montenegro, North Macedonia, Bosnia & Herzegovina) when speaking of prevention of violent extremism.

2. VIOLENT EXTREMISM IN THE WESTERN BALKANS

2.1. SERBIA – CASE STUDY

In Serbia, different forms of violent extremism and terrorism can be identified. During the past several decades, Serbia has been intensively combatting ethnic separatist terrorism and extremism in the territory of Kosovo and Metohija, as well as in the southern part of Central Serbia (Preševo, Bujanovac, Medveđa).[9)]

[8)] See more in: USAID. 2011. *The Development Response to Violent Extremism and Insurgency: Putting Principles into Practice*, Washington DC: USAID, p. 2-3. Accessed at: https://www.usaid.gov, 12.06.2022.

[9)] For several years, Serbia combatted the terrorist organization UÇK, which acted in the territory of the Serbian province Kosovo and Metohija, only to have these ethnic separatist tendencies spread to the southern part of Central Serbia as well through actions of the "Liberation Army of Preševo, Bujanovac and Medveđa".

Besides that, Serbia also faced some problems regarding religiously funded terrorism linked to Syrian and Iraqi battlefields, which were joined by 49 of adult Serbian citizens (Petrović & Stakić 2018) who became members of some of the terrorist organizations present in these fields.[10)] With the *COVID-19* pandemic, hand-in-hand with the migration crisis, came along the intensification of the extreme right-wing, which is increasingly on the rise. It is interesting noting that, in Serbia, the extreme left-wing is also increasingly becoming strong (predominantly as a response to social problems and a reaction to the extreme right-wing), even though it has been marginalized during several past years.

The Criminal Law of the Republic of Serbia recognizes several criminal acts related to terrorism.[11)] In October 2014, a Law on Amendments of the Criminal Law of the Republic of Serbia (Official Gazette of the Republic of Serbia No. 108/2014) was adopted, thus introducing two new criminal acts into Criminal Law:

- "Participation in a war or an armed conflict in a foreign country", Article 386a,
- "Organization of participation in a war or an armed conflict in a foreign country", Article 386b.

These provisions refer to individuals who illegally participate in a war or an armed conflict on the territory of a foreign country, and the Office of the Higher Public Prosecutor is in charge of their implementation. On the other hand, provisions presented in Article 393a of the Criminal Law apply to individuals who joined terrorist organizations, for which implementation the Prosecutor's Office for Organized Crime is in charge. It is important stressing that Serbia is the only country in the Western Balkans region to differentiate FTF (Foreign Terrorist Fighter) and FF (Foreign Fighter), which is in accordance with the UN Resolution No. 2396.

When speaking of a strategic framework, Serbia passed a National Strategy for prevention and combatting terrorism for the period from 2017-2021.[12)] In the strategy, the four most important fields are separately defined: (1) Prevention of terrorism, violent extremism and radicalization that leads to terrorism; (2) Protection through detection and removal of threats from terrorism and other vulnerabilities in the protection system; (3) Criminal prosecution of terrorists, with respect to human rights, rule of law and democracy and (4) Response of the system to a terrorist attack.

[10)] It is believed that the majority of people joined the terrorist organization called the "Islamic State".

[11)] "Terrorism", Article 391; "Public incitement to conducting terrorist acts", Article 391a; "Recruitment and training for conducting terrorist acts", Article 391b; "Financing terrorism", Article 393; "Terrorist association", Article 393a.

[12)] At the time being, the new strategy is being created.

In an institutional sense of the word, P/CVERLT in Serbia falls to the jurisdictional specter of the National Coordination Body for Prevention and Combatting Terrorism (hereinafter: National Coordination Body). This Body was formed by the Government's Decision passed in 2019, and in the same Decision, the National Coordinator was defined. The National Coordination Body has 26 members and is consisted of representatives of the most significant ministries, as well as representatives of security services of the Republic of Serbia.

2.2. MONTENEGRO – CASE STUDY

Until nowadays, two criminal proceedings were conducted in the Higher Court of Montenegro relating to the criminal act of participation in foreign armed formations, in line with Article 449b of the Criminal Law of Montenegro.[13)] Since 2012, a total of 23 adult Montenegrin citizens departed to Syria, while five individuals (Đorić 2020, 9)[14)] participated in the Ukrainian battlefield (Đorić 2020, 9). Besides that, ethnic nationalist extremism was been noted to be on the rise for the last several years in Montenegro as well.

The main role in prevention of violent extremism in Montenegro is given to the National Operational Team (NOT)[15)], as well as the National Coordinator for Prevention of CVE.[16)] NOT is divided into several RAN groups: RAN 1 for communication and narratives; RAN 2 for education and youth; RAN 3 for local communities; RAN 4 for health and social protection; RAN 5 for police and other law enforcement authorities; RAN 6 for prisons and probational punishments; RAN 7 for exit strategies.

Violent extremism and terrorism are recognized in the Strategy for National Security as methods of fulfilling political and other goals that directly impact vital and strategic interests of the state. Moreover, violent extremism is also recognized in the Strategy of Defense of Montenegro, while the issue of prevention of terrorism is also treated within the Strategy for prevention and combatting terrorism,

[13)] One proceeding reffers to the Syrian, and the other to the Ukrainian battlefield.
[14)] All five of them returned.
[15)] Within NOT, a Team for Help and Protection is formed as well, consisting of representatives of relevant subjects that are members of the National Operational Team. The role of Team for Help and Protection is enabling efficinency in action.
[16)] This title is nowadays expanded, and thus we are speaking of a National Coordinator for the fight against violent extremism, terrorism, money laundering and terrorism financing.

money laundering and terrorism financing. The phenomena of violent extremism and radicalization are dealt with in detail in the **Strategy for prevention of violent extremism 2016-2018**, as well as in the complementary Action Plan. This strategy was adopted in December 2015, and the competent body for creation of the Strategy was the Ministry of Justice.

The Bureau for Operational Coordination and Harmonization of Activities of Organs of the Intelligence and Security Sector controlled the measures of the Action Plan for implementation of the CVE Strategy for the period of 2016-2018.

Within NOT, a **Team for Help and Protection** was formed as well. With the goal of promotion of work, institutional strengthening and linking, as well as providing systemic response and approach to every single case, NOT initiated formation of the **Team for Help and Protection**. This team is consisted of representatives of relevant subjects, all members of the National Operational Team, for the purpose of rational and efficient conduct.

In 2021, with the change in Government, Montenegro formed a **National Interdepartmental Operational Team for Prevention of National Extremism and Terrorism**, thus spreading the existing focus from violent extremism to terrorism as well.

2.3. NORTH MACEDONIA – CASE STUDY

According to official data, a total of 156 citizens of North Macedonia departed to the Syrian and Iraqi warzones (Spasovska 2022). This explicitly points to the fact that this state has, for several years now, been facing the issue of religiously motivated extremism and terrorism.[17)] Besides that, North Macedonia has for several years been hit by ethnic separatist terrorism, to which testifies the terrorist attack conducted in 2015 in Kumanovo by Albanians originating from the territory of Kosovo and Metohija. Having in mind all of the above, the fight against radicalization and violent extremist is one of the top priorities of the Government of the Republic of North Macedonia.

[17)] One of the most extensive actions that resulted in arrests of extremists and terrorists was organized in 2016 (best known under the codename "Ćelije") in Struga, Gostivar, Kumanovo and Skopje, when returnees from foreign battlefields who were preparing for new attacks were arrested.

The Republic of North Macedonia falls to the specter of countries which have separate strategies for violent extremism and terrorism, that were simultaneously passed for the period of 2018-2022. Besides these two strategies, the phenomena of violent extremism and terrorism are also dealt with in the National Strategy for Fight against Money Laundering and Terrorism Financing.

Within the Criminal Law, a criminal act of participation in foreign armies, police, paramilitary and parapolice formations (Art. 322-a) is separately treated. Besides that, there is also a criminal act treating the act of terrorism (Art. 394-b), as well as the criminal act of "terrorist threat to constitutional law and security" (Art. 313).

The main state institution that deals with the issue of violent extremism is the National Committee for Prevention of Violent Extremism and Fight against Terrorism, founded for the first time in 2017.

2.4. BOSNIA AND HERZEGOVINA – CASE STUDY

Bosnia and Herzegovina is burdened by numerous political problems, among which are violent extremism and terrorism as well. During several past years, this state faced significant problems related to religiously funded terrorism, having in mind that, according to official data, between 250 and 300 citizens of Bosnia and Herzegovina departed to battlefields in Syria and Iraq.[18)] According to other sources, this numbers rises up to 360 people, and thus, it is difficult to define precisely the exact number.[19)]

Until nowadays, a total of 62 adults and 22 children returned to B&H, while eight children whose parents are citizens of B&H or who originate from B&H returned to other countries. Currently, in the territory under control of the (predominantly) Kurdish Syrian Democratic Forces (SDF), a total of 52 citizens of B&H can be found in local prisons and camps.[20)] In cooperation with the US, the first group of 25 citizens of B&H returned in December 2019 (seven men, six women and 12 children).[21)]

[18)] See more in: SRNA. October 19, 2022. Na povratak sa ratišta čeka još 82 državljana BiH. Accessed at: https://lat.rtrs.tv, 23.10.2022.
[19)] See more in: Kešmer, M. December 3, 2021. Četverogodišnji dječak porijeklom iz BiH nastradao u kampu Al-Hol u Siriji. Accessed at: https://www.slobodnaevropa.org, 15.08.2022.
[20)] See more in: SRNA. October 19, 2022. Na povratak sa ratišta čeka još 82 državljana BiH. Accessed at: https://lat.rtrs.tv, 23.10.2022.
[21)] See more in: Kešmer, M. January 8, 2021. Bh. državljanke u sirijskim kampovima: Pominje li nas iko? Accessed at: https://www.slobodnaevropa.org, 27.10.2022.

The B&H Strategy for Prevention and Fight against Terrorism for the period of 2015-2020 stresses that the comprehensive goal is to prevent all forms of extremist and terrorist actions, respecting the values of democracy, rule of law and human rights and freedoms.

The sub-goals presented in the Strategy are the following:

1. Prevention of hate crimes, radicalism and terrorism in all forms;
2. Protection of critical infrastructure;
3. Promotion of investigation and criminal prosecution procedures when speaking of acts of terrorism and familiar criminal acts;
4. Response/reaction to possible terrorist acts and remediation of their consequences.

The Strategy also defines the tasks of the Ministry of Security of Bosnia and Herzegovina, which are especially stressed in the following strategic measures:

5.1.13 (Creation of programs of resocialization of individuals charged with conducting criminal acts of terrorism or participation in paramilitary formations);

5.1.18 (Participation in prevention of violent extremism and terrorism on an international level) and

5.3.4 (Identification and processing of potential and existing members of extremist and terrorist groups).

In 2014, B&H adopted the Law on Amendment of the Criminal Law of B&H (that is, Article 162b.), used for sanctioning departure to foreign battlefields and participation in foreign paramilitary organizations. Soon enough, the Council of Ministers of Bosnia and Herzegovina adopted an Information on Citizens of Bosnia and Herzegovina who are situated in the conflict zones in Syria and Iraq, with the goal of their repatriation. The main role in this process is given to the Ministry of Security of Bosnia and Herzegovina, as well as the Coordination Team.

The Coordination Team is consisted of the most significant institutions in the state, namely the Prosecutor's Office of Bosnia and Herzegovina, the Ministry of Foreign Affairs of Bosnia and Herzegovina, Ministry of Civilian Affairs of Bosnia and Herzegovina, Ministry of Human Rights and Refugees of Bosnia and Herzegovina, the State Agency for Investigation and Protection, the Border Police of Bosnia and Herzegovina, the Direction for Coordination of Police Bodies,

Federal Bureau of Police, Ministry of Interior of the Republic of Srpska, Police of the Brčko District of Bosnia and Herzegovina, etc. Apart from the previously listed institutions, the competent authorities of entity and cantonal bodies in the field of social protection, education and health are engaged as well.

In the draft[22)] of the Strategy for the Fight against Terrorism in B&H for the period of 2021-2026, for the first time is it explicitly stressed that right-wig extremism (referred to in this document predominantly as ethnic nationalism) poses a serious threat to the security of this state. Moreover, a close link of the extreme right-wing to football hooligan groups and certain clerical structures is mentioned as well.

CONCLUSION

Through comparative analysis of the presented four case studies (Serbia, Montenegro, North Macedonia, Bosnia and Herzegovina), the most significant strategic documents and institutional approaches to prevention of violent extremism are identified. What can be concluded at first glance is the fact that countries of the Western Balkans are synchronized when speaking of strategic and institutional approaches to combatting violent extremism. It is not a rare occurrence that examples of good practice found in one country are quite successfully (with more or less alternations) being used in other countries of the region as well. This was especially noticeable during the period of 2014/2015, when all countries of the Western Balkans criminalized the act of departure to foreign battlefields (which corresponded with the war in Syria and Iraq, but also with events in Donbas). Some countries (such as Serbia), in accordance with the UN Resolution No 2396, clearly differentiated foreign terrorist fighters (FTF) from foreign fighters (FF), that is, a distinction was made between the criminal act of "Terrorism" (Art. 391) and "Participation in war or armed conflict in a foreign country" (Art. 386a). In other countries of the region, these two occurrences are often equaled. It is interesting to mention that in many democratic countries in Europe, as well as world-wide, participation in foreign battlefields is not explicitly defined as a criminal act, and thus, the countries of the Western Balkans made a step forward.

[22)] The adoption of the new Strategy was set in motion in 2021.

When speaking of taking strategic actions, two approaches can be distinguished:

1. There is one strategy treating jointly phenomena of violent extremism and terrorism, and
2. Two different strategies are being created – one for extremism and one for terrorism.

Having in mind the previously acquired experience, it seems that the future trend will revolve around treating violent extremism and terrorism within one strategy.

In many countries, the strategies expired during the *COVID-19* pandemic, and thus the creation of new strategic documents was prolonged due to technical problems (inability to organize direct contact, online communication, etc.), as was the case with Serbia, while in some other countries, due to lumbering and complex governing systems (as was the case of Bosnia and Herzegovina), the process was slowed down.

What emerged as an evident trend is that the new strategies will have much more space dedicated to the right-wing (that is, ethnic nationalist) extremism in comparison to previous documents, which corresponds with strengthening of the extreme right-wing, not only on a global level, but in the Western Balkans region as well. There is an assumption that the *COVID-19* pandemic, as well as the migration crisis and the war in Ukraine, will additionally intensify the issue of the extreme right-wing.

When speaking of institutions, in all countries, the key roles were given to the ministries of force (usually the Ministry of Internal Affairs), while in a more personal approach, this task is given to the National Coordinator (P/CVE coordinator) who, in some countries, deals solely with violent extremism, while in others (for example, in Montenegro), that official deals with terrorism as well. It is obvious that, in the future, the role of the National Coordinator will be unified in order to treat both violent extremism and terrorism, due to natural overlapping of these phenomena.

In the context of old and new challenges, it can be said that religious extremism is still present, having in mind that more than 400 individuals originating from the Western Balkans are currently still being held in Syria and Iraq.[23)] The post-conflict heritage (referring to the wars of the nineties of the previous century) is still a well-known, old topic for the countries of this region, which can easily result in national tensions. Having in mind the effect of the coronavirus pandemic on the global plan, the so-called *covid-related extremism* can be expected, with a power to unite the extreme left-wing and the extreme right-wing, especially when speaking of anti-globalism (which is a common enemy to both fractions). With an increasing energy and economic crisis correlating with the war in Ukraine, the Western Balkans might even become a stage of social protests, which will certainly create a new problem with the extreme left-wing as well.

The final conclusion is that the Western Balkans region is quite unstable due to mutual disagreements from the past, but also the new challenges to be faced in the future. Maybe the countries of the Western Balkans should be a little bit wiser and learn from the mistakes made during their difficult and dynamic joint history. Given that every crisis nurtures various forms of extremism, it is possible that the new multiplied crises will represent a fertile ground for some new toxic ideologies. Only through joint coordination in the field of prevention of violent extremism and terrorism, as well as joint learning from good (and bad) practices can countries of this region be ready to face new security challenges.

[23)] See more in: Kešmer, M. May 27, 2022. BiH prvi put ima strategiju za suzbijanje desnog ekstremizma. Accessed at: https://www.slobodnaevropa.org, 23.10.2022.

REFERENCES

1. Đorić, Marija. 2014. Ekstremna desnica, Nauka i društvo, Beograd, pp. 134-135.
2. Đorić, Marija. 2020. Priručnik za prepoznavanje, prevenciju i suzbijanje radikalizacije i nasilnog ekstremizma kod učenika, Biro za operativnu koordinaciju – Nacionalni operativni tim, Podgorica.
3. Kešmer, M. December 3, 2021. Četverogodišnji dječak porijeklom iz BiH nastradao u kampu Al-Hol u Siriji. Accessed at: https://www.slobodnaevropa.org, 15.08.2022.
4. Kešmer, M. January 8, 2021. Bh. državljanke u sirijskim kampovima: Pominje li nas iko? Accessed at: https://www.slobodnaevropa.org, 27.10.2022.
5. Kešmer, M. May 27, 2022. BiH prvi put ima strategiju za suzbijanje desnog ekstremizma. Accessed at: https://www.slobodnaevropa.org, 23.10.2022.
6. OSCE. December 7, 2012. DECISION No. 1063, OSCE CONSOLIDATED FRAMEWORK FOR THE FIGHT AGAINST TERRORISM. Accessed at: https://www.osce.org, 23.02.2019.
7. OSCE. 2014. *Sprečavanje terorizma i borba protiv nasilnog ekstremizma i radikalizacije koja vodi ka terorizmu: Pristup putem rada policije u zajednici*, OSCE, Vienna.
8. OSCE. 2020. *A Whole-of-Society Approach to Preventing and Countering Violent Extremism and Radicalization That Lead to Terrorism*, OSCE, Vienna.
9. Petrović Predrag & Stakić Isidora. 2018. Extremism Research Forum: Serbia report, British Council, Belgrade. Accessed at: https://www.britishcouncil.rs , 22.09.2022.

10. Perry, Valery (ed.). 2019. Extremism and violent extremism in Serbia: 21st-Century Manifestations of an Historical Challenge, ibidem-Verlag, Stuttgart.

11. Schmid, Alex. 2014. Violent and Non-Violent Extremism: Two Sides of the Same Coin?, International Centre for Counter-Terrorism (ICCT) – The Hague.

12. Spasovska, Zorana Gadžovska. October 5, 2022. Makedonska vlada objavila 'crnu listu' ljudi koji se bore u Siriji. Accessed at: https://www.slobodnaevropa.org, 05.06.2022.

13. SRNA. October 19, 2022. Na povratak sa ratišta čeka još 82 državljana BiH. Accessed at: https://lat.rtrs.tv, 23.10.2022.

14. Stepić, Milomir. 2012. Zapadni Balkan: primer geografskog raspojmljivanja i geopolitičkog manipulisanja. *Nacionalni interes*, no. 3, pp. 9-34.

15. UNDP. 2016. PREVENTING VIOLENT EXTREMISM THROUGH PROMOTING INCLUSIVE DEVELOPMENT, TOLERANCE AND RESPECT FOR DIVERSITY. Global Meeting, 14-16 March, 2016, Oslo. Accessed at: https://www.undp.org, 01.02.2022.

16. USAID. 2011. *The Development Response to Violent Extremism and Insurgency: Putting Principles into Practice*, Washington DC: USAID, p. 2-3. Accessed at: https://www.usaid.gov, 12.06.2022.

17. Wither, James Kenneth. 2016. "Salafi – Jihadists: A Threat to the Western Balkans?", In: Violent Extremism in the Western Balkans, edited by Filip Ejdus and Predrag Jureković, Collection of papers presented at the PfPC workshop held in Belgrade.

Gordana Paović Jeknić*)
Sonja Tomović-Šundić**)
Ivan Jeknić***)

UDC: 316.647.7:340.13(497.16)
323.28:340.13(497.16)
316.647.7:17.023

LEGAL AND ETHICAL ASPECTS OF VIOLENT EXTREMISM AND TERRORISM

Abstract: *The paper explores the legal and ethical dimension of violent extremism and terrorism in the contemporary world, with special consideration pertaining to Montenegro. The fundamental concept of the paper is to analyze the process and content of legislation and strategy regulating this occurrence in society, in both national legal systems and international law, with the aim of determining in what ways sanctions and preventive measures in politics affect the occurrence of different forms of extremism. Furthermore, the paper argues the significance of ethical theories and the study of ethics as a subject in the education system of a country in preventing the onset of violent extremism in later times. Extremism is tied to ideologies openly opposed to the moral values of principles of democracy, rule of law, universal human rights and personal liberties, including the respect of differing opinions. Within that context, the roles of legal and moral norms are especially important for prevention of violence as a means of achieving goals which are political, economic, religious or nationalistic, by nature. Additionally, the paper explores the characteristics of the social environment that strengthen the resilience of the individual to radicalization and adoption of extremist views and aspirations, and extremist ideological messages and belief systems.*

Keywords: *legal norms, ethical values, violence, resilience, extremist ideology.*

*) PhD, Faculty of Law, University of Montenegro

**) PhD, Faculty of Political Sciences, University of Montenegro

***) LLM, Faculty of Political Sciences, University of Montenegro

INTRODUCTION

In the recent decade, there has been a significant increase in extremism in European countries and globally. Extremism as a notion is often associated with terrorism, although they do not completely coincide. What connects these two notions is violence. The growing influence of extremist ideologies undermines the democratic heritage of a country and its political culture, and when extremism turns into violence, human lives are also at risk. Consequently, a strong and appropriate response from the state and society is needed in order to prevent and counter the emergence and development of extremist ideologies and values, and their escalation into violence and terrorism. In other words, it is necessary to develop society's resilience to the emergence of extremism. Achieving these goals starts from two aspects, which imply the application of different methods and means. The first is legal, which must include the political, institutional and security capacities of a state. The second is moral – ethical, which includes the values and ideas nurtured by a community – citizens, and the relationship of their political culture to extremism.

1. LEGAL ASPECT OF VIOLENT EXTREMISM AND TERRORISM

In legal and political theory and practice, there are attempts to expose the phenomena of extremism and terrorism, in order so that we, as a society, can counter them, that is, with the aim of condemning these phenomena and behaviours which pose a threat to our security, but above all, to prevent their occurrence in society, because they violate not only legal norms, but also the highest moral values. In this context, extremism in the broadest sense represents a certain extreme, "a behaviour and thinking on the border of what is permissible with a tendency to cross that border, which is contrary to the legal, customary and cultural norms of a society" (Đorić 2016, 22). A more destructive type of extremism, harmful to the state, is called violent extremism. It differs from non-violent extremism, which remains only on the level of a recognizable dangerous value system, primarily when it comes to the use of violence in practice. More precisely, violent extremism primarily implies violent acts for the purpose of religious, ideological or political goals. The usual pyramidal structure of these extremist groups consists of: the leader – the person at the top, the members – activists ready to implement the planned activities, and supporters – followers and sympathizers (Đorić 2016, 20 – 21).

The question arises why the majority agrees that extremism is an unacceptable and harmful phenomenon for democracy, stability, the rule of law, i.e., for the human rights and freedoms in a state. Primarily because it can turn into terrorism, or more precisely when we take a closer look, basically every form of terrorism has an element of extremism and was born from it. In fact, extremism and terrorism are often mistakenly equated, although it is clear that terrorism is a political concept, because it has political motives, political goals and political negative effects, while extremism can appear in all spheres of social and political life, from religion, culture, to sports and, finally, in politics. In this sense, in theory, terrorism, as a phenomenon known for centuries, is observed through politically motivated violence directed against a certain government, in order to achieve political goals by applying various means and methods while inducing fear, threatening and intimidating (See: Đorić 2020, 13), or through the use of illegal violence to induce fear, with the intention of coercing and intimidating the government or a society in order to achieve political, religious or ideological goals (See: Hrabar 2012, 281).

Investigating its original meaning, the word *terrorism* itself originates from the Latin word *terror* and means fear, horror, dread, etc. In this sense, we could say that different authors tried to define the occurrence of terrorism, although it has long been a globally recognizable problem with an emphasized emergent element of aggressiveness, depending on which aspect of terrorism special emphasis had been given to. Thus, the definition of terrorism given by Brian Jenkins is the one most often mentioned in the literature. He believed that "terrorism is the use or threat of the use of force aimed at achieving political changes". Following the genesis of terrorism, it is necessary to point out the historical fact that the word *terrorism* (in the context of so-called modern terrorism, in contrast to the previously recorded religious terrorism) appeared practically for the first time during the French civil revolution among the Jacobins, who imposed a dictatorship over the population. The goal at the time was to use the so-called reign of terror to force people to recognize and live under the rule of a smaller number of people and to work in their interest. Mass terrorism, which experienced its expansion in the 20th century and its ubiquity in the 21st century, seems to be present daily in its cruellest sense, as evidenced by the availability and

the spread of the media and the internet on a global scale. In this context, we agree that the turning point in the global fight against terrorism in the world was the terrorist attack on the USA in 2001, which is often considered by the public as the tragic event that changed the whole world (See: Marić 2012, 89-91).

When it comes to Montenegro and its fight against these dangerous and undesirable phenomena and specific security challenges, in numerous government documents in the field of prevention and countering violent extremism, the starting point is the conclusion that the problems of violent extremism and terrorism, which are used as methods for realizing political and other goals, can result in collapse and destruction of national, strategic and vital interests. Accordingly, in order to eliminate them, the state must make all administrative and technical capacities available, ensure good coordination of all entities of the security system, and especially international cooperation (National Security Strategy of Montenegro, 8-13). The National Security Strategy of Montenegro and the Defence Strategy of Montenegro point to the fact that these security problems are part of a broader regional and global security threats and risks, and that it is necessary to effectively implement all necessary measures and activities to fight against terrorism at all levels, and against further radicalization, recruitment and financing of terrorism (National Security Strategy of Montenegro 2018, 13; Defence Strategy of Montenegro 2019, 5). Thus, in accordance with the Strategy for Countering Violent Extremism 2016-2018 and the accompanying Action Plan, the National Operational Team for the Implementation of the Action Plan for the Implementation of the Strategy for Countering Violent Extremism was formed, which was given the mandate to prepare a new strategy for the prevention and countering violent extremism for the period 2020-2024. Therefore, the Government of Montenegro, on February 6, 2020, adopted the Strategy for Prevention and Countering Radicalization and Violent Extremism for the period 2020-2024, stating in it that various forms of violent extremism and radicalization are global problems that the state must actively and efficiently confront, both at the local, central, regional and interstate levels. To this end, as emphasized by the Government of Montenegro, it is necessary to increase the resilience and capacities of the society, empower institutions and strengthen the international

position of Montenegro in the fight against these dangerous and harmful phenomena. Therefore, it should be taken into account that we are in the sensitive area of the Western Balkans, burdened by the mortgage of wars from the end of the 20th century, the target of various geo-strategic interests and influences, with the evident and increasingly present hate speech in the media, social networks, i.e. the internet as a whole, even individual cases of ethno-nationalist radicalisation, which all require decisive, comprehensive and successful action and countering such undesirable and dangerous phenomena (See: Strategy for Prevention and Countering Radicalization and Violent Extremism for the period 2020-2024, 2020, 6; Please note that the problem of terrorism prevention is also analysed in the Strategy for the Prevention and Countering Terrorism, Money Laundering and Terrorism Financing, as well as in the Cyber Security Strategy of Montenegro).

It should be noted that this Strategy was created on the basis of numerous relevant international documents: starting from guidelines and resolutions of the United Nations, reports and communications of the European Commission, EU policies and priorities for the relevant sectors, to the decisions, programs and guidelines of the Council of Europe and the OSCE, etc. The Strategy highlights the special importance of Resolution 2242 of the United Nations Security Council on the necessity of states' more efficient and persistent fight against terrorism and violent extremism, whereby great importance is given to preventive activities and measures, in accordance with the principles and values of the Charter of the United Nations, the Universal Declaration of Human Rights and other international documents and mechanisms for the protection of human rights and freedoms in modern states (See: Strategy for Prevention and Countering Radicalization and Violent Extremism for the period 2020-2024 2020, 3-6). Furthermore, it is important to emphasize that the General Assembly and the Security Council of the United Nations have adopted decisions stating that the drivers of violent extremism are the following: weak socio-economic opportunities, discrimination and marginalization, violations of human rights and freedom, radicalization influenced by injustices, abuses and tensions. That is why the United Nations proposes preventive measures aimed at dialogue and conflict resolution, strengthening good governance, gender equality, education, employment and human rights and

freedoms, as well as the rule of law, etc. Additionally, the Strategy follows the standards of the European Union and is harmonized with the Joint Action Plan on Counter-Terrorism for the Western Balkans (Tirana, 2018). It foresees the common goals that should be achieved by the countries of the Western Balkans in order to eliminate terrorism and prevent the emergence of violent extremism. Starting with the creation of a strong legal and institutional framework, through the exchange of information, operational cooperation, strengthening the capacity to fight money laundering and financing of terrorism, to the protection of citizens and infrastructure. Finally, the main goal of the Strategy is the need to "increase the resilience of society, better response of institutions and stronger international position of Montenegro in the fight against radicalism and violent extremism" (Find more: Strategy for Prevention and Countering Radicalization and Violent Extremism for the period 2020-2024 2020).

The fact stated in the Strategy is that the Western Balkans region is a particularly sensitive area due to different geo-strategic interests and influences, recent wars and divisions in society. Thus, in the Report of the European Commission on Montenegro (2019), it was determined that Montenegro is marginally threatened by the emergence of radicalization and foreign fighters (in this sense, 23 persons left for Syria from 2012-2018, and two criminal proceedings were conducted in the Higher Court due to the suspicion that certain persons participated in foreign armed forces. They have served prison terms. Find more: Strategy for Prevention and Countering Radicalization and Violent Extremism for 2020-2024 2020, 6-11). Additionally, the Police Directorate, assessing threats from violent extremism, believes that, in Montenegro, there is no risk of greater violent extremism that would affect human rights and freedoms, although it is clear that this threat is very real and requires preventive, systemic and strategic measures. All this should be taken even more seriously in the light of unstable geopolitical events, which were primarily caused by the war in Ukraine and continuous individual terrorist attacks in various parts of the world. Factors that influence radicalization are different: starting from structural (political events at the regional and global level, violation of human rights, corruption and lack of responsibility, etc.), then individual (influence of religion, social exclusion of

individuals, desire to acquire financial benefits, etc.), to enabling access to weapons, as well as access to social networks in order to access radicalized groups – the so-called enabling factors (Strategy for the prevention and suppression of radicalization and violent extremism for the period 2020-2024 2020, 6-8 – Situation Analysis; For Montenegro, the criminal court proceedings for attempted terrorism from 2016, in which certain leaders of political parties, were highlighted).

In accordance with the Law on basic principles of intelligence and security sector in Montenegro, a National Operational Team was formed, which is responsible for the implementation and monitoring of the Strategy and relevant action plans. Furthermore, in 2021, a National Coordinator was appointed and a National Interdepartmental Operational Team was formed to counter violent extremism, terrorism, money laundering and terrorist financing. The authorities of the European Commission for countering terrorism, in addition to supporting this National Operational Team and Montenegrin efforts for the prevention of violent extremism and countering terrorism, especially emphasize the constant need to fight against all forms of radicalism and violent extremism, which are increasingly present in the Western Balkans countries. Finally, a large number of conferences that were organized in Montenegro (with the support of international organizations, the Government and embassies of Western European countries, etc.) were also in the function of the fight against violent extremism and radicalism, because the European future of Montenegro, European values and strong institutions are the best way for the Montenegrin society to provide an adequate response to these dangerous and negative phenomena.

The Criminal Code of Montenegro, within the framework of crimes against humanity and other goods protected by international law, stipulates, among others, in Article 447, the criminal offence of terrorism, then public instigation to commit terrorist acts (Article 447a), recruiting and training to commit terrorist acts (Article 447b), financing of terrorism (Article 449), terrorist association (Article 449a), participation in foreign armed forces (Article 449b) and others (Criminal Code of Montenegro 2020).

The Law on Prevention of Money Laundering and Financing of Terrorism in Montenegro regulates measures and actions aimed at detecting and preventing money laundering and financing of terrorism, as well as the powers and work of the organizational unit of the Ministry of Internal Affairs (Financial Intelligence Unit) that performs tasks aimed at preventing money laundering and financing of terrorism (Law on Prevention of Money Laundering and Terrorist Financing 2021). The following is, in particular, considered as terrorist financing in the context of this Law: providing or collecting or an attempt of providing or collecting funds or property, in any way, directly or indirectly, with the intention or with the knowledge that they may be used, in their entirety or in part, for preparation or execution of a terrorist act by terrorists or terrorist organizations. Additionally, encouraging or assisting in providing or collecting the aforementioned funds or property, etc (Law on Prevention of Money Laundering and Terrorist Financing 2021).

2. MORAL ASPECT OF VIOLENT EXTREMISM AND TERRORISM

The answer to the question of how violent extremism arises should contain a multidisciplinary interpretation and consideration from the point of view of different scientific disciplines, primarily humanistic ones. Obviously, one of the reasons why our historical era can be considered as a civilization at risk is found in the emergence of ideologically motivated violence with the goal to achieve social, economic, religious, political and other goals. Although it is a security challenge, we can study violence in the modern world not only as a political and social problem, but also a moral one, because basically it is about not abiding to not only legal regulations, but to universal ethical values as well. Also, in this way, a broader framework can be established for action in the direction of countering and prevention of the causes of violent extremism and terrorism as its ultimate form of manifestation. As we can see, this negative practice of *solving* social issues is present even in the age of highly developed technology and economic development in modern political communities. In a way, violent extremism has a transnational

character, so its appearance on the historical scene must be explained in terms of its causes, methodology and goals for the world in which we live in. At the same time, it has national, regional and widest global significance for the global community. In this context, we will try to shed light on the phenomenon of violent extremism in its various dimensions, in order to have a more comprehensive understanding of its principles, guided by the ancient ideal that understanding is the first step in solving problems, and knowledge is the basis of preventive action.

Primarily, it is necessary to analyse:

1. The phenomenology of violence;
2. The ideology of violence and dogmatism as a methodology for creating individuals' fanatical consciousness;
3. The function of morality in limiting violent extremism; and
4. Whether it is possible to control a crisis.

In order to explain the phenomenology of violence in the world of global-institutional connection, we will use anthropological findings, since anthropology is a philosophical discipline that studies humans, human nature and societies. Aristotle defined a man as *zoon politikon*, according to which sociality is the fundamental determination of human nature, the basis of our differentiation in relation to the animal world (See: Aristotle 2017). A human is a political being, insofar as he has a *logos* (mind), so that in the axiological sense he can evaluate experiences, from the point of view of moral values as good and evil, and due to this property, he is capable of creating a human community. At the basis of the philosophical understanding of Aristotelianism, trust in the rationality of human nature, the power of philosophical reasoning, is emphasized. Reason uses dialectics, which can be used to acquire conceptual principles and knowledge of principles, as norms of moral behaviour. Philosophy as a theoretical discipline served the establishment of moral behaviour and the establishment of practical philosophical disciplines: ethics and politics. In this context, only a spiritually developed human can serve the interests of the state and be a good citizen in order to participate as actively as possible in the public life of a *polis*.

According to this, the political culture in Ancient Greece rested on the moral formation of one's personality and education of citizens for participation in social life.

However, the fundamental rationale of modernity arose from the denial of the connection between ethics and politics, freeing up space for *the legitimization* of violence, because political goals are seen as something *above* moral and legal regulations. In this context, violence has a utilitarian character, it is connected with the realization of political demands of certain groups that want to seize social power.

Hannah Arendt developed a thesis that violence, in contrast to power, force, strength and authority as the most important political concepts, is connected with the means necessary for its execution (See: Arendt 2002). Additionally, violence should be considered in relation to human nature. In Hobbes' thesis that a man in his natural state is evil, subject to interests, innate nature and instincts, we find a basis for the assumption that good and evil are much more deeply rooted in man's psychological structure than we could conclude if we adhere to the ideas of humanistic philosophy. In any case, we can look for the origin of evil as a lever of destruction in interpersonal relations in philosophical, anthropological, psychological, social and historical reasons, but also in the politically formed ideology of violence. Judging by everything, we can state the view that violence, despite the technological development of modern civilization, is still present on the social scene, is connected to technical means of destruction, while its character is connected to the anthropological nature of the human individual. Its main feature is unpredictability. Violence resists control, it is interested in the destruction of established power, striving to establish violent practices as a correct model of social life. Only power obtained through democratic procedures has legitimacy and is politically responsible, because it is based on elections, the rule of law and the institutions of the political order. Ultimately, using the means of violence, one cannot maintain or create a new form of power in the long term (Arendt 2002, 9), insofar as only a weakened power uses violence, while legitimacy itself collapses through the use of illegal means: "Violence can destroy power and is completely incapable of creating it" (Arendt 2002, 4).

Accordingly, violence can only stop the erosion of power in the short term, which has been delegitimised using undemocratic methods. Here we can refer to the theoretical considerations of the utilitarians, their revitalization of the concept of utility, and the rule that encourages citizens to listen only to those decisions of the Government, which are morally justified (See: Mill 2000).

Obviously, the causes of violent extremism in the modern world can be considered using the theoretical postulates of different scientific fields. Supporting violence as a way of solving political problems, or participating in ideologically motivated violence, can first of all be interpreted as illegal ethical behaviour, which violates moral norms and universal values. A quasi-political culture, based on the abuse of religion and politics, represents a paradigm on which the ideology of violent extremism rests.

First of all, ideology is based on fanaticism and dogmatic exclusivity among its supporters. Radical attitudes are based on the ideology of evil, the violation of moral principles, and pseudo-religious and pseudo-political explanations that have all the characteristics of a mythical consciousness. There is a strong emotional feeling, which is forced with the over-dimensioning of national, religious or political *endangerment*. This promotion of violent practice introduces all forms of destruction, even terrorist actions for the sake of achieving the *holy goals* in the future. Extremism in theoretical learning, the belief in the superiority of one's own religious or ethnic affiliations, leads to disturbances in thinking and violent practices among its amassed supporters, because they have lost the qualities of critical thinking and individuality as a result of indoctrination. As the main problem for the emergence of violent extremism, we cite ideological education, the creation of a totalizing consciousness, amassing and propaganda from the centres of power, created so to transform its members into reliable instruments for the execution of violence. When part of a large mass of people, a person does not respect moral considerations, thus losing the features of a free person and his/her responsibility. In fact, a person, shaped to carry out ideological tasks, loses accountability, bowing to the collective authority that he/she unquestioningly serves: He/she is ready to

achieve extreme goals with extreme means (See: Arendt 1994). It is a total disruption of political activity in public life. If we are talking about the radical right, whose rise in modern European states is worrisome, dogmatic attitudes, symbols, theoretical constructs become the backbone of their political program, which serves to impose their own views on social problems: "The whole meaning of an amassed man is a demonstration of force, which is vividly manifested by its members, because they, in a state of delirium and elevated temperature, bewitched as if in a magical ritual, loudly express their political ideas" (Tomović Šundić 2022, 246).

To summarize, in shaping non-democratic individuals, various means of ideological manipulation, political and national myths, symbols, convictions, beliefs and dogmatic teachings calculated to awaken emotionality and abolish individual opinion, are being used. This is the preparation for loyalty, and the creation of obedience-based psychology. In the glossary of the security culture, extremism represents a methodology that forms a tendency towards excessive, extreme and irreconcilable attitudes, a division to *us* and *them*, *traitors* and *righteous*, where the harshest punishments are foreseen for dissenters. Like *the Myth of the Cave* in Book VII of Plato's *State*, the blind adherents of an ideology are prisoners in a dark catacomb that symbolizes the darkness of ignorance, governed and directed by *invisible* branches of power. For the Ancient Greeks, barbarians were all nations that did not belong to the Hellenic culture; in the modern world, neo-barbarism is an effort to cancel all differences: national, religious, ethnic, in order to rule more easily with a homogenized mass of like-minded people. Thus, instead of a free society, the ideal of national cohesion is postulated, instead of truth – loyalty, instead of justice – utility, instead of solidarity – selfish interests. A person without moral culture and conscience becomes a dangerous tool for achieving the *proclaimed* goals. He/she rejects the value-based political order, not respecting legal and moral norms, convinced of the correctness of only his/her truth, denying the same right to members of more violent ethnic, political or religious groups. Politics as an ideology is actually a doctrine of mastering social processes, while forcing dogmatic thinking and taking control over the social order and its institutions.

Finally, the role of moral education that would be carried out in the educational system, the introduction of ethics as an important discipline for the formation of free citizens, is an important social strategy in the creation of a democratic political culture (See: Strauss 2006). It is the work on shaping new patterns of political behaviour, in order to weaken the arguments for the emergence of violent extremism and terrorism, by strengthening moral awareness based on the principles of tolerance and mutual understanding. This is a way to show extremist theories not only wrong, but opposed to truth and morality, as well as disastrous for the public interest, as well as for individuals. The thing to keep in mind is that ideological *brainwashing* is not only politically useless, but also immoral, since such an individual is actually thoughtless and uneducated. Violence against consciousness, as well as violent practices, sooner or later proves to be fruitless. History still hasn't denied that violence has not solved any social problem in the long term; it actually just resulted in an enormous increase in the amount of destruction: "Violence can only produce violence, but violence has never solved a political problem" (Bentham 1948).

This is why we can understand the problem of violent extremism as a whole if we analyse its ethical and anthropological aspect more comprehensively, since the bearers of these negative practices are persons as individuals, unprepared to respect human dignity. They were educated to deny the fundamental moral categories: fairness, goodness, beauty, truth, which as cardinal virtues had a prominent place even in the ancient times. Also, the ethics of duty, inspired by Immanuel Kant's categorical imperative, could provide us with a satisfactory answer, because we are obliged to preserve world peace and the global community not only as an economic or legal order, but as a community of free individuals. Therefore, public good, solidarity, moral awareness and responsibility, the enhanced role of the humanities, can be important answers to the challenges we face in the modern world.

In our civilization at risk, it is necessary to ask ourselves whether we can control the crisis as a fundamental political and security problem, as well as how to avoid Machiavellianism as a style of behaviour in positions of power (See: Christie 1970). Global connectivity should not rest only on the profit of capital, but the purpose (*telos*) of our civilization should have a moral dimension. This means responsibility in order to put our technological development and economy into the function of not only transnational business, but of achieving a fairer distribution of social wealth. In order to survive, integration is necessary, based on the common goals of all actors on the social scene, with the belief that politics and economics depend on people.

In this context, our resilience to violent ideologies should be based on democratic institutions, but also on conscious individuals – personalities resilient to various forms of dogmatism. It is about resilience to the imposed image of the world, which reduces an individual to a mere consumer. Anthropology of personality implies a conceptual framework based on knowledge and moral concepts, which do not allow the transition to ideological extremism, and ultimately violence. In order for the consciousness to become fanatical, the individual must be uneducated, confused in ethical terms for non-ethical action.

To summarize, all forms of extremism rely on indoctrination of consciousness, by creating a totalizing pattern of behaviour, which remains hermetic to different interpretations. For this purpose, an ideology of violence is necessary, which has a simplified structure of a myth that is worshipped uncritically. However, whether we consider the causes (deontology) or the consequences (utilitarianism) of the moral law, from the point of view of deontological ethics, violence is not allowed in any single case. Regardless of democratic rhetoric, violence always destroys and collapses the safety and security of all members of a society. This security aspect in the creation of democratic political communities remains the key to eliminating instability, dealing with the relationship between the strong and the weak, geopolitical aggravation along the lines of the East-West conflict. Obviously, in divided political cultures, clientelism and partial interests of political and economic elites undermine the security aspect and world peace (See: Zuboff 2019).

Dealing with crises, political confrontations, extremism, which above all endanger citizens, is a moral task, a challenge to strengthen our physical and spiritual immunity. To that extent, our common goal is a global community in which there is a security system, in which citizens are protected and can lead a morally correct life. Disruption in the value system, the collapse of the idea of progress, all this favours the creation of a civilization of fear, insecurity, lack of freedom, and that is why ensuring peace, security and stability is an increasingly difficult task in the face of growing problems.

Finally, resistance to every form of violent ideologies and extremism should be established as a political and ethical goal, the mode of existence of democratic political communities. The *new* political culture should be based on universal concepts, as the best form of resistance to the creation of a collectivist paradigm. Personal and general security, as well as the stability of the international order, should be based on a philosophy of peace, in which there is no room for relativizing moral concepts and their value equalization. Classical disciplines – anthropology and ethics – can serve in the renewal of the humanistic impulse of our civilization, a conceptual framework for social, economic and moral revival (see: Foucault 1980). Strenghtening the trust in the rule of law, respect for the human right to moral dignity and living in fair communities, in order to reduce violence to a minimum, and create awareness of zero tolerance for violent practices. If in the end we deliberate seriously about what our common interest is, which has political and the widest social implications, it is reasonable to conclude that moral behaviour is the *conditio sine qua non* of overall prosperity, individual and collective security, the purpose of existence of human communities. In other words, our highest interest is not to act self-interested. This therefore means working for the common good. The public sphere should be taken not only as an area of pragmatic expression of partial purposes, but as a community in which stability is achieved by non-violent means. For these reasons, the phenomenology of violence cannot be properly studied without appreciating the potential of a scientific view of the world that comes from the sphere of moral philosophy.

CONCLUSION

The reasons and causes of the emergence of violent extremism and terrorism are different, from difficult social and economic conditions of citizens, to weak institutional and political capacities for resistance to geopolitical and economic turmoil (economic crisis, migration, wars, etc.). Although the causes are different, the consequences are very similar, if not identical, in many parts of the world. Extremist ideologies very easily turn into violence and terrorism, which endanger the lives of citizens, and disrupt political stability and destroy the value-based cohesion of society – the rule of law, human rights and freedoms, and moral (ethical) values of citizens. In order to develop resistance to these phenomena, it is necessary to engage not only the institutional and legal power of the state, but also ethical values in the political culture of a developed modern society (morality, solidarity, justice, human rights and freedoms) – the values and norms of society and the state.

REFERENCES

1. Arent, Hana (Arendt, Hannah) 1994. *Istina i laž u politici (Truth and Politics)* Belgrade: Filip Višnjić.
2. Arent, Hana (Arendt, Hannah) 2002. *O nasilju (On Violence)* Belgrade: Nova srpska politička misao.
3. Aristotel (Aristotle) 2017. *Metafizika (Metaphysics)* Belgrade: PAIDEIA, Službeni glasnik (PAIDEIA, Official Gazette)
4. Bentham, Jeremy. 1948. *An introduction to the Principles of Morals and Legislaton*. New York: Macmillan.
5. Criminal Code of Montenegro. 2020. Official Gazzete of the Republic of Montenegro, no. 70/2003, 13/2004 – amended and 47/2006 and Official Gazette of Montenegro, no. 40/2008, 25/2010, 32/2011, 64/2011 – oth. law, 40/2013, 56/2013 – amended, 14/2015, 42/2015, 58/2015 – oth. law, 44/2017, 49/2018 and 3/2020.
6. Đorić, Marija. 2016. *Ekstremna levica: ideološki aspekti levičarskog ekstremizma*. Belgrade: Institut za političke studije.
7. Đorić, Marija. 2020. *Priručnik za prepoznavanje, prevenciju i suzbijanje radikalizacaje i nasilnog ekstremizma kod učenika (Manual for recognition, prevention and countering radicalization and violent extremism among students)*. Podgorica: Nacionalni operativni tim (National Operations Team).
8. Fuko, Mišel (Foucault, Michel) 1980. *Istorija ludila u doba klasicizma (Madness and Civilization: A History of Insanity in the Age of Reason)* Belgrade: Nolit.
9. Christie, Richard, Geis, Florence. 1970. *Studies in Machiavellianism*. New York: Academic Press.

10. Hrabar, Sandra. 2012. *Politički terorizam i ekstremizam u zapadnoj Evropi u drugoj polovini 20. stoljeća (Political terrorism and extremism in Western Europe in the second half of the 20th century) Rostra*, Vol. 5, No 5, 281-286. Zadar: University of Zadar.

11. Law on Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro no. 033/14, 044/18, 073/19, 070/21.

12. Marić, Silvana. 2012. *Terorizam kao globalni problem (Terrorism as a global problem), Medianali*, vol.6, no. 11, 87-102. Zagreb 2012.

13. Mill, John Stuart. 2000. *M. De Tocqueville on Democracy in America*. Chicago: University of Chicago Press.

14. Tomović Šundić, Sonja. 2022. *Čovjek je političko biće (Man is a political being)* Podgorica: Nova knjiga.

15. Strategija nacionalne bezbjednosti Crne Gore (National Security Strategy of Montenegro) 2018. Government of Montenegro. https://www.gov.me.

16. Strategija odbrane Crne Gore (Defense strategy of Montenegro) 2019. Government of Montenegro. https://www.gov.me.

17. Strategija prevencije i suzbijanja radikalizacije i nasilnog ekstremizma za period 2020-2024 (Strategy for Prevention and Countering Radicalization and Violent Extremism for the period 2020-2024) Government of Montenegro.

18. Strauss, Leo, Cropsey, Joseph (ur.). 2006. *Povijest političke filozofije (History of political philosophy)* Zagreb: Golden Marketing – Tehnička knjiga.

19. Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for u Human Future at New Frontier of Power*, New York: Public Affairs.

Zoran Keković*)
Tanja Milošević**)

UDC: 314.151.3-054.73(569.1:497-15)
314.151.3-054.73(581:497-15)
314.151.3-054.73(477:497-15)

PERSPECTIVES OF MIGRATION CRISIS IN THE WESTERN BALKANS: COMPARATIVE ANALYSIS OF THE CASES OF SYRIAN, AFGHAN AND UKRAINIAN REFUGEES

Abstract: *Since the beginning of the 21st century, the old continent has been facing the biggest surge of refugees, reaching a breaking point in 2015, when Europe greeted about 1.3 million of Syrian refugees. Since the year of 2015 will forevermore be remembered as the beginning of the Syrian migration crisis, the year of 2021 will remain marked by the fall of the Afghan state and the takeover of power by the Taliban, resulting in a big influx of Afghan refugees to Europe. Unfortunately, the following year of 2022 did not provide a relief for Europe, having in mind the launching of the Russian military intervention in Ukraine, which resulted in yet another driver for migration and seeking refuge world-wide, and in the Balkans as well. Throughout all these crises, the Balkan route emerged as one of the most significant transition points of many refugees, being the final destination to some of them. Having all this in mind, in this paper, the authors will present an analysis of these three separate migration crises, with a special emphasis on unique characteristics of the arrival, reception and the future perspective of Syrian, Afghan and Ukrainian refugee communities in the Western Balkans. Thus, the aim of this paper is to provide a comprehensive analysis of the current state, as well as the future perspectives of these three contemporary refugee nations, with a special emphasis on the impact of the influx of Syrian, Afghan and Ukrainian refugees on political, economic and security situation in the Western Balkans. With the use of methods of data collection and content analysis, as well as scientific observation and description, the authors will answer the main research question of this paper, thus confirming the hypothesis stating that active conflicts pose a political, economic and security threat to countries world-wide, given that they represent quite strong drivers for mass migrations of population residing in conflict zones. Moreover, the author will also conduct semi-structured interviews with prominent stakeholders and first responders to the migration crisis in the Balkans, namely interpreters and cultural mediators engaged in the field, in order to provide a comprehensive representation of the true impact of mass migrations on political, economic and security changes in the Western Balkans.*

Key words: *migration crisis, Western Balkans, refugees, Syria, Afghanistan, Ukraine*.

*) Professor at the Faculty of Security Studies of the University of Belgrade.
**) PhD candidate at the Faculty of Political Sciences of the University of Belgrade; registered UNHCR interpreter for Arabic, English and French.

INTRODUCTION

The first modern humans – *homo sapiens*, evolved from their early hominid predecessors about 200,000 to 300,000 years ago, predominantly in Eastern and Southern Africa. About 70,000 to 100,000 years ago, these first humans started migrating from Africa into Eurasia, slowly populating region by region. Little by little, the human race conquered the planet. Thus, we can say that the human kind owes its geographical omnipresence to – migration.

For thousands of years, humans have moved around the globe for many reasons – "in search for food, in flight from enemies, or in pursuit of riches, spreading their cultures, languages, diseases and genes" (Ferrie & Hatton 2013, 2). Nowadays, the idea of migration still remains imprinted into human conscience, and the 'root causes' for migration are the same. Namely, it is a known fact that the main causes of contemporary migration are predominantly conflicts and harsh economic situation[24)]. These two drivers also potentially distinguish migrants from refugees, even though both categories deserve the right to decent living conditions and a chance for good life.

The International Organization for Migration (IOM) differentiates several typologies of individuals residing or attempting to reside in a foreign country. The broadest term – **alien**, represents 'an individual who does not have the nationality of the State in whose territory that individual is present' (Sironi et al. 2019, 8), and is most often found to be present in the said territory illegally. Aliens can be both migrants and refugees, whilst the term **migrant** is a broader 'umbrella term, not defined under international law, reflecting the common lay understanding of a person who moves away from his or her place of usual residence, whether within a country or across an international border, temporarily or permanently, and for a variety of reasons. The term includes a number of well-defined legal categories of people, such as migrant workers; persons whose particular types of movements are legally defined, such as smuggled migrants; as well as those whose status or means of movement are not specifically defined under international law, such as international students' (Sironi et al. 2019, 132). Apart from clearly defined terms

[24)] The common stance present in the academia regarding causality of migrations reiterates that the majority of big movements of people are, apart from harsh economic situation and ongoing conflicts, predominantly conditioned by demographic explosion (especially when speaking of Africa) and social engineering (especially when speaking of Asia and Latin America).

immigrants (defined as individuals moving into their country of arrival from their country of origin) and **emigrants** (defined as individuals moving from their country of origin to a different country), the most common typology of migrants represents **economic migrants**. Even though economic migrants do not represent a category in international law, this term refers to individuals that are moving or have 'moved across an international border or within a State, solely or primarily motivated by economic opportunities' (Sironi et al. 2019, 61). **Migrants** can be a product of forced or voluntary migration. However, the most vulnerable category present within any migration crisis – **refugees**, are predominantly forced to leave their countries of origin. In this sense, a refugee is being defined as 'a person who, owing to a well-founded fear of persecution for reasons of race, religion, nationality, membership of a particular social group or political opinion, is outside the country of his nationality and is unable or, owing to such fear, is unwilling to avail himself of the protection of that country; or who, not having a nationality and being outside the country of his former habitual residence as a result of such events, is unable or, owing to such fear, is unwilling to return to it' (Sironi et al. 2019, 171). Finally, both migrants and refugees are given a chance to seek asylum and thus be qualified as **asylum seekers**, that is, individuals seeking international protection. 'In countries with individualized procedures, an asylum seeker is someone whose claim has not yet been finally decided on by the country in which he or she has submitted it' (Sironi et al. 2019, 14). However, it is important noting that **not every asylum seeker will consequently be recognized as a refugee, but every recognized refugee is automatically eligible to be an asylum seeker**. Moreover, it is a common occurrence that people who move out of conflict zones are initially labeled as 'refugees'; however, it must be noted that not every individual originating from a conflict zone is in fact a refugee, and many, as it will be seen in the case of the Syrian migration crisis in Europe, decide to leave their home countries not because the conflict is directly affecting their lives and their wellbeing, but because a country collapsed by war is not able to offer them the life they wish for themselves. Thus, it can be said that contemporary conflicts most often cause migrations, both voluntary and involuntary, and both serve as catalyzers of big influxes of both migrants and refugees. Economic hardship, also a common cause for migration of people, is yet another result of political and security instability in the country, and thus, it can be noted that outbreak of conflicts and economic hardship, in this sense, go hand-in-hand.

Big movements of peoples have often followed great instabilities, and the modern society is no stranger to big influxes of foreign nationals seeking better living conditions in another man's country of origin. In the era of democracy and respect of human rights, most countries of the world have engaged the first responders, that is, legal and humanitarian professionals, as well as medical, security and border police units, in order to provide the best assistance possible to this vulnerable category of individuals. Namely, 'while other countries defended themselves from the 'invasion' of migrants with barbed wires, walls, and different legal solutions, Serbia left its doors wide open and expressed a human dimension, which is often forgotten in the times of a crisis' (Đorić 2017, 43). The same was the case with the majority of countries of the Western Balkans. In 2015, the entire region was hit by the most pronounced ever influx of (predominantly illegal) migrants, originating from the Middle East and Africa, that used the Balkan route as their passageway towards Europe. The 'Syrian migration crisis' was pronounced over in 2019; however, little did we know that it was the first of a series of migration crises to emerge, caused predominantly by ongoing conflicts and political instabilities world-wide.

1. CONTEMPORARY MIGRATION CRISES

Given the frequency of occurrence, as well as its impact and consequences world-wide, and especially in the Western Balkans, special attention should be paid to defining the term '**migration crisis**'. According to the International Organization for Migration (IOM), migration crisis represents a 'complex and generally large-scale migration flows, as well as the mobility patterns caused by a crisis that can often lead to considerable vulnerabilities for affected people and communities, and pose serious management challenges in the longer term' (Tantaruna August 30, 2019). A migration crisis can be sudden or gradual, caused by natural or man-made causes, and can 'take place internally or across borders' (Sironi et al. 2019, 137). The term 'migration crisis' has been dominantly present

in the public discourse in the Western Balkans since 2015, when the region registered intensification of influx of migrants and refugees originating from numerous Middle Eastern and African countries, but predominantly from Iraq, Syria and Afghanistan. The said crisis, lasting for almost five years – from 2015 to 2019, is nowadays known as the 'Syrian migration crisis', given that the most prominent group among migrants and refugees consisted of Syrian nationals escaping the ongoing conflict and atrocities conducted by the so-called Islamic State, a terrorist organization active in Syria, as well as in Iraq. At the time already present in migration flows through the Balkans towards Western Europe – the Afghan migrants were well present in the region, even long before the beginning of the 'Syrian migration crisis'. Namely, according to the annual report for the year of 2012, produced by the Serbian Ministry of Interior, the majority of illegal immigrants crossing the borders and entering Serbia were of Afghan and Pakistani origin (Bjelica & van Bijlert August 5, 2016). Soon enough, after the retreat of the US Army from Afghanistan and consequent rise to power of the Taliban in August 2021, the exodus of Afghans intensified, and Europe, as well as the rest of the world, was faced with yet another 'migration crisis' – 'the Afghan migration crisis'. Faced with a reoccurring phenomenon, the world reacted differently in this case, and thus provided us with another methodology of response to human catastrophe and fear for life. Namely, two countries of the region emerged as 'the great saviors' of the Afghan refugees – Albania and North Macedonia, as well as the so-called "Kosovo", providing instantly the American administration with quotas of refugees they are able to temporarily 'rescue', before they continue their journey to the United States. The rest of the Western Balkans, worn out by the previous consistent migrant flows, remained silent, already taking care of the Afghan nationals arriving to the region prior to Taliban takeover, as well as the ones continuously arriving illegally through the Balkan route.

Finally, less than a year later, the launch of the Russian intervention in February 2022 served as yet another driver for migration, leaving the Western Balkans region, traditionally close to Russia and Ukraine, faced with intensified

influx of migrants and refugees from both countries. This ongoing conflict has caused the biggest migration crisis in Europe since the end of the World War Two, resulting in more than seven million of Ukrainians leaving their country of origin, of whom the majority fled to the surrounding countries, and some found their way to the Western Balkans as well. Given the fact that the conflict in Ukraine is still ongoing, the number of displaced individuals will only continue to rise. Having in mind that six months of Russo-Ukrainian conflict generated more refugees than the entire 'Syrian migration crisis', which resulted in about 6.6 million displaced Syrians, the 'Ukrainian migration crisis' can be officially proclaimed the biggest migration crisis of the 21st century.

In all three scenarios, the Western Balkans served as a significant crossroads for many migrants and refugees travelling towards Western Europe. Namely, throughout 2015 and the first half of 2016, the Balkans served as the main migration route for Syrian, Iraqi, Afghan and all other migrants and refugees. Some of them continued their journeys towards various final destinations, while the others remained in migrant camps throughout the region. In 2021, in the surge of another migration crisis consisted of Afghan refugees fleeing the Taliban rule, Albania, North Macedonia and the so-called "Kosovo" – all previously a part of the Balkan route, accepted a significant amount of Afghan refugees, while the other countries of the region continued to register illegal border crossings of Afghan nationals, as well as refugees and migrants from other nations, on their way to Western Europe. And finally, since February 2022, all Western Balkan countries lent a helping hand to the arriving Ukrainian refugees, hosting more than 140,000 individuals from the affected region. Having in mind the current state of the world politics, as well as the fact that migration crises, wherever occurring in the world, tend to affect the Western Balkans region, the following chapters will provide an analysis and assessment of the causes of the given crises, as well as the reception of migrants in the Western Balkans, reaction of the public and the state, and finally future perspectives of the said refugee nations present in our region.

1.1. SYRIAN MIGRATION CRISIS

In 2011, the Arab world was shaken by a series of social uprisings, globally known as the 'Arab Spring'. In Syria, faced with the same discontent of popular masses, president Bashar al Assad believed that the Syrian social unrest could be 'put to rest' with the use of force. However, the social unrest turned into a revolution, revolution turned into violence, and violence turned into civil war. Busy with fighting against the opposition forces, Bashar al Assad left a blind eye to the rise of a terrorist organization that will soon enough change the climate in the entire region – the so-called Islamic State. By 2014, the Islamic State 'held about a third of Syria and 40 percent of Iraq' (Wilson Center 2019), and became the main menace to society and humanity in both Syria and Iraq. Soon enough, rivers of refugees and migrants from Syria started flooding Europe, and the Western Balkans as well.

Nowadays, more than a decade after the beginning of the Syrian civil war, 'Syrians constitute **the largest forcibly displaced population globally**' (Doumit 2021, 680), with an estimated 6.6 million refugees, predominantly situated in Turkey, as well as in European countries. At the moment, Turkey alone is hosting a total of 3.7 million registered Syrian refugees (UNHCR February 2022), while the rest settled predominantly in developed countries of in Europe. However, on their way to Western Europe, the majority of Syrians still ended up seeking at least temporary refuge in Turkey and Greece, before continuing their travels. Some of them still remain in these countries, as well as in the countries along the Balkan migration route. The said passage is still active, with a recorded intensification of border crossings in the region due to travel restrictions imposed as preventive measures against the coronavirus pandemic. According to FRONTEX, 'the Western Balkan route was the second most-used path to Europe as the detections of illegal border crossings more than doubled in 2021 to a total of 61,735' (FRONTEX n.d.).

The main final destinations for Syrians in Europe were Germany and Sweden, who still host the largest group of Syrian refugees – more than half a million of Syrians settled in Germany, while Sweden hosted a little bit over 100,000 Syrian

nationals (Doumit 2021, 682). Given that the Balkan route served as the biggest migration corridor towards Western Europe in 2015 and 2016, and that North Macedonia 'was the first to face the mass inflows of migrants' (Oruc et al. 2020, 6), the countries along this route almost instantly started establishing detection system in order to grasp the given situation, following the example of North Macedonia. By December 2015, migration management system was fully functional, 'recording all people on the move' (Oruc et al. 2020, 7) in all Balkan countries. The first responders in the migration crisis, notably the security forces, legal counsel, humanitarian workers and medical staff, soon enough established practices and humanitarian points along the route, thus enabling provision of humanitarian aid to the best level possible.

Still, the **reception** of Syrian refugees remains ambiguous, though it varied during the last decade from full understanding and provision of humanitarian aid with empathy, to intensification of anti-immigration attitude among the public and strengthening of far-right and nationalist sentiments. Namely, even though the Syrian refugee crisis began in 2011, the international community became aware of the suffering of the Syrian people around 2015, 'once the refugee flow began to reach European borders at increasing rates' (Doumit 2021, 680) and when the first victims, depicted in the three-year-old Alan Kurdi drowning in an effort to reach Greece, started taunting the world. At the given moment, many countries of the world, led by the United States, launched a Global War on Terror on one side, and established humanitarian corridors on the other. The first Syrian refugees were met with understanding, whilst the majority of asylum seekers were in fact granted asylum in their wished country of final destination. However, with the surge of **terrorist attacks** on European soil, and notably the ones conducted by followers of the so-called Islamic State, conducted in France, Belgium, Germany, the United Kingdom and Spain since 2015 onwards, the public sentiment has shifted from sympathy to discontent, gradually building towards ultra-nationalist notions of the migration crisis colored by anti-Semitism, anti-Muslim and anti-racism. Thus, we have witnessed **securitization** of the migration issue, at which point the question of accepting a refugee from a Muslim country was equaled by many with putting one's own nation and wellbeing of the local population at risk.

1.2. AFGHAN MIGRATION CRISIS

In 2001, the US military intervention in Afghanistan weakened the position of the predominantly Pashtun Islamic fundamentalist group named Taliban, forcing it to regroup in the neighboring Pakistan. Less than ten years later, the Taliban began taking back the lost territory little by little, only to take over the entire country by August 2021. As the country slowly sunk into chaos, mass exodus from Afghanistan began as well, forming vast waves of refugees, predominantly towards the United States and EU member states. In this case, the main **cause** for the massive surge of Afghan refugees was and still is the Taliban regime, given that the activities of this group have also served as strong drivers for migration even before the overtake of power in the country. The Balkan route, formerly the main geographical crossroad for many migrants and refugees travelling towards Western Europe, once again served as a helping hand in yet another migration crisis.

Afghan refugees were no strangers to the Balkans even before the Taliban takeover of the country, given that they represented **the second largest group of migrants** present in the region (Reka October 14, 2021). Namely, in 2015, when over a million of people travelled through the Western Balkans, almost 250,000 of them originated from Afghanistan, and by the end of the year, Afghans accounted for about 20 percent of all arrivals to Europe (Bjelica & van Bijlert August 05, 2016). The following year, the common criteria was established between Austria, Slovenia, Croatia, Serbia and Macedonia, defining the circumstances under which someone fled their country of origin as a determinant that ended up enabling free passage to Iraqi and Syrian refugees, but not the Afghans, who were predominantly perceived to be voluntary migrants, in search of better economic conditions (Bjelica & van Bijlert August 05, 2016). This decision left hundreds of Afghan nationals stranded in many countries of the Western Balkans, thus deeming them as ‘second class migrants’, hidden in the shadows of the great Syrian suffering.

However, in 2021, when the Taliban took over the country, many countries world-wide, led by the United States, begun evacuation of their nationals from Afghanistan, whilst the US government attempted to evacuate all Afghan nationals linked and employed with American governmental and non-governmental organizations as well. Such practice was soon enough adopted by all countries world-wide with any kind of governmental or non-governmental organizations present in the country. Moreover, more than 100 countries pledged to accept Afghans fleeing Afghanistan, among which were Albania, North Macedonia and the so-called "Kosovo", while Serbia and Montenegro 'said no to the U.S. request' (Reka October 14, 2021). At the given moment, 'Albania, one of Europe's poorest countries, agreed to take in up to 4,000 Afghan refugees permanently. Kosovo will welcome up to 2,000 and North Macedonia up to 2,000 persons' (Reka October 14, 2021). Upon the arrival of Afghan refugees, hotels and student centers were allocated for this purpose in Albania and North Macedonia[25)], while in the so-called "Kosovo", the Afghans settled near the KFOR/NATO base. In the final countdown, Albania hosted and is still hosting some of the 2,400 Afghan refugees in waiting for US visas, of whom '150 have now left on flights to the United States and several other EU countries' (Marusic et al. December 17, 2021). By the end of 2021, North Macedonia ended up hosting a total of 407 Afghan refugees, '76 of whom have already left for three different countries' (Marusic et al. December 17, 2021), notably France, Ireland and Greece. The remaining bunch is predominantly settled in hotels near Skopje. Finally, in the so-called "Kosovo", a total of '971 Afghans have been placed there in two refugee camps' (Marusic et al. December 17, 2021).

Besides 'regularly accepted refugees' settled in Albania, North Macedonia and the so-called "Kosovo", humanitarian workers engaged in various Western Balkans countries state that the Balkan route has been reactivated and has thus

[25)] These hotels and student centers are located in Durres and Shengjin.

become 'the only viable alternative for people on the move as member states like Greece and Italy have fortified their borders and the Central Mediterranean route grows increasingly deadly' (ECRE January 21, 2022). Namely, Afghan refugees are still present and still constitute the most dominant migrant nationality in the majority of Western Balkans countries, though the method of **reception** has slightly shifted during the course of the last decade.

In the beginning of the mass migration crisis attributed to intensification of arrival of Syrian refugees to Europe, the main focus of humanitarian organizations was directed towards Middle Eastern migrants, and predominantly Syrians and Iraqis. Therefore, in the first months of the crisis, the majority of humanitarian workers, and especially interpreters and cultural mediators, were predominantly skilled to communicate in Arabic, whilst languages and dialects such as Dari, Farsi and Pashto were not that common among humanitarian professionals. Due to language barrier and necessity of using English when communicating with Afghan (and Pakistani) refugees and migrants, the initial crisis response was limited, in waiting for the first assimilated asylum seekers to begin working along the scarce Farsi interpreters of Serbian origin. However, currently, the majority of Western Balkan states have skilled linguistic teams proficient in Farsi, Dari and Pashto, not only academically trained, but also armed with live skills acquired in the field, given that the majority of interpreters for these language combinations started engaging in the field instantly after graduation.

Unfortunately, skills alone are not sufficient for successful crisis management when speaking of migration crises. Even though more than 100 states world-wide decided to host Afghans fleeing the Taliban rule, many EU states remained silent or even stressed the need 'to defend Europe from illegal migration', still in fear of reoccurrence of yet another 'Syrian migrant crisis' dressed in the national flag of Afghanistan. Namely, France and United Kingdom initially proposed 'the creation of a United Nations-run safe zone in Kabul' (Mammone September 04, 2021),

while some European far-right politicians securitized the new migration crisis, pointing to the fact that the migration routes might be used by the Taliban and other extremist groups for reaching Europe and possibly conducting terrorist attacks. Such statements intensified anti-immigration attitudes among public, thus dividing Europe into humanitarians and extreme rightists. Having in mind the already present growing anti-migration sentiments towards migrants and refugees that appeared following a series of terrorist attacks on European soil, negative attitudes towards another migration crisis in Europe, now centered on Afghan refugees, did not come as a surprise, especially since the Afghans have long been present along the migration routes.

Apart from the present anti-migration sentiments, it is worth noting that acceptance of Afghan refugees, to some extent, has become **politicized**, given that providing security, especially to former US collaborators and local staff of Afghan origin, served as a good identifier of pro-US and pro-NATO stance. By providing shelter to Afghans, these countries proved that they are the true allies of the US, and thus strengthened or at least attempted to strengthen their ties to the American government.

1.3. UKRAINIAN MIGRATION CRISIS

In February 2022, the Russian Armed Forces launched a military intervention in Ukraine, thus setting off the largest conflict in Europe since the World War Two. Rooted in separatist tendencies of Crimea and Donbas dating back from 2014, this continuing conflict grew into a full-scale war, thus causing vast movements of people in the region, first within the territory of Ukraine, then into neighboring countries and beyond, to the rest of the world. For the time being, this conflict has resulted in displacement of more than seven million Ukrainians from their country of origin, of whom the majority fled to the surrounding countries.

The Russian Federation played a significant role in providing refuge for Ukrainians, given that almost 2.5 million of Ukrainians are currently residing in this neighboring country that is apparently, in this case, being both part of the problem and part of the solution. The next biggest number of Ukrainian refugees was recorded in Poland, currently hosting about 1.3 million of Ukrainians. Slovakia, given its geographical proximity to Ukraine, provided refuge to a little over 90,000 people, while Romania is currently hosting almost 56,000 and Hungary almost 30,000 Ukrainians. When speaking of the Western Balkans region, a total of 142,835 Ukrainian refugees and migrants were recorded in seven countries of the region, whilst, as of August 30, Bulgaria was hosting a little bit over 77,000 of people, followed by Montenegro, a country that provided refuge to 24,482 people. Serbia is currently hosting around 17,458 Ukrainians, while Croatia is hosting 17,487 of them. Finally, a small portion of Ukrainian refugees settled in North Macedonia (3,296), Albania (2,780) and Bosnia and Herzegovina (218) (UNHCR August 30, 2022). Given the present situation, humanitarian response teams were established in countries of the region, whilst in Serbia, governmental and non-governmental organizations engaged in the field were joined by linguists skilled in both Ukrainian and Russian language in order to provide efficient response to the current Ukrainian migration crisis. Still, given that Ukrainians, as well as Russians, are traditionally present in the Balkans, the 'Ukrainian crisis' was not perceived in the public eye as a 'migration crisis', but as slightly intensified influx of Ukrainian citizens to the region.

Given the nature of arrival of Ukrainian refugees to the region, as well as the fact that, in this case, we are speaking of the arrival of Christian refugees, many scholars have reiterated that 'this is not Europe's first refugee crisis, but it is different, as a comparison with 2015 shows. The size and speed of the exodus are one sign, but so is the European Union's perception that this time it's different. Geographical proximity is an obvious distinctive feature: a far-off conflict is not the same as one taking place on the continent itself' (Garcés March 2022), whilst the majority of European politicians stated that Ukrainian refugees are not the

refugees Europe is used to – **they are Europeans**. If reading between the lines, we understand that 'this time these refugees are welcome, and the reason is not just their urgent need for international protection, but because they are Europeans, Christians, "civilized" and middle-class' (Garcés March 2022). And finally, this time around, as a consequence of the 'good image' of Ukrainian refugees, the European borders remained and will remain open, contrary to the case during the Syrian and the Afghan migration crisis.

The previously described attitude, as well as the fact that Ukrainians were previously able to travel to the majority of European countries for the period of 90 days without a visa, enabled the creation of a quite intense influx of middle- and upper-class Ukrainians, who soon enough found their place in the European real estate market by purchasing and leasing apartments and houses privately, thus raising the housing prices throughout the region, and especially in Serbia and Montenegro. This new development thus gravely impacted economic situation in the country, especially given the fact that housing prices in several countries have risen to previously unrecorded levels. Such trend has been recorded in almost all countries affected by a bigger influx of Ukrainian refugees, which was the case with Poland as well, where 'the demand for apartments for rent has spiked in the large Polish cities that have been the refugees' main destination' (Rzhevkina April 22, 2022).

CONCLUDING REMARKS

Big movements of people have never in history been conditioned by positive economic, political and security factors, but has most often risen from the need for better living conditions and even the need of protecting one's own life. In this sense, big migrations of people indeed deserve to be called 'crises', affecting not only the countries of origin of migrants and refugees, but the countries of final destination as well.

The initial hypothesis of this paper stating that migration crises, and especially increased influx of Syrian, Afghan and Ukrainian refugees all have great impact on political, economic and security situation in the Western Balkan has been proven through examination of the three presented migration crises. Namely, the first of the three crises – the Syrian migration crisis, however initially met with empathy and understanding, soon ended up being perceived by the receiving countries as a significant security threat. The securitization of the Syrian migration crisis especially enhanced following the series of terrorist attacks in Europe attributed to the so-called Islamic State, after which the ultra-nationalist and anti-migrant sentiments rose to the fore, thus making the already difficult situation the Syrian and other refugees were in even more difficult.

The second migration crisis came along with coming of the Taliban regime to power in Afghanistan in August 2020, causing havoc and panic among Afghan nationals trying to leave the country. Given the strong American presence in the country and the withdrawal of the US Army from Afghanistan preceding the rise of the Taliban, the 'Afghan migration crisis' ended up being used as leverage in negotiations and strengthening position and relations with the US administration, as we have seen on the example of North Macedonia, Albania and the so-called "Kosovo" accepting significant quotas of Afghan refugees in waiting for a US visa. Moreover, the previously induced anti-migratory attitudes present in the European public, despite strong interest of certain countries for provision of aid to Afghan refugees, remained quite strong, and the majority of Afghan refugees remained neglected and stranded on European borders due to the fact that they come from a poor, Muslim country.

Finally, the 'Ukrainian crisis' serves as the best example of prioritization of nationality among migrant and refugee nations, given the fact that the Ukrainian refugees are world-wide perceived firstly as Europeans, then as Christians, and lastly as (favored) refugees. In this sense, we can even speak of a sort of favoritism

among migrants, since many countries than previously closed their frontiers before the Syrian and Afghan migrants nowadays greet the Ukrainian refugees with open hands, lifting visa requirements and enabling special conditions for the new wave of migrants. However, this open-door policy slightly backfired, causing significant economic problems in host countries, notably the rise of housing expenses and the prices in the real estate market throughout Europe.

However different, all three examples of migration crises represent outcomes of serious security, political and economic insecurities in one part of the world causing similar outcomes in the other through displacement of vast numbers of people. In the Gospel of Matthew, it is said that 'violence begets violence'. In this case, violence does not necessarily beget violence; however, it can be concluded that crisis (often) begets crisis, whether of security, political or economic nature, whether serious or mild.

REFERENCES

1. Bjelica, J. & van Bijlert, M. 2016. "Afghan Exodus: The opening and closing of the Balkan corridor". *Afghanistan Analysts Network*, August 5, 2016. https://www.afghanistan-analysts.org.
2. Doumit, J. 2021. "The Syrian refugee crisis, ten years later: how the United States can improve its response". *Georgetown Immigration Law Journal*, Vol. 35, pp. 679-686.
3. Đorić, M. 2017. „Migrantska kriza kao generator levičarskog i islamističkog ekstremizma u Evropi". *Politička revija*, godina (XXIX) XVI, Vol 51, no. 1/2017, pp. 39-54.
4. ECRE. 2022. "Balkan Route: Movement Increases in the Region as Europe Fortifies, Afghans Fleeing the Taliban Face Dire Conditions at EU Borders". *ECRE*, January 21, 2022. https://ecre.org.
5. Ferrie, Joseph; Hatton, Timothy J. 2013. "Two Centuries of International Migration". *IZA Discussion Papers*, No. 7866, Institute for the Study of Labor (IZA), Bonn.
6. FRONTEX. n.d. "Migratory Routes: Western Balkan Route". https://frontex.europa.eu.
7. Garcés, B. (March 2022). "Why this refugee crisis is different". *CIDOB opinion*.
8. Mammone, A. 2021. "Europe is politicizing Afghan refugees instead of helping them". *Al Jazeera*, September 04, 2021. https://www.aljazeera.com.
9. Marusic, Sinisa Jakov et al. 2021. "Afghan Refugees Slowly Leave Balkan Countries for West". *Balkan Insight*, December 17, 2021. https://balkaninsight.com.

10. Oruc, N. et al. 2020. *The Western Balkan Migration Route (2015-2019)*. Analytical Report. International Centre for Migration Policy Development, Vienna, Austria.

11. Reka, Blerim. 2021. "The role of the Balkans in the Afghan refugee crisis". *GIS*, October 14, 2021. https://www.gisreportsonline.com.

12. Rzhevkina, A. 2022. "Influx of Ukrainian refugees stokes housing shortage in Poland". *Notes from Poland*, April 22, 2022. https://notesfrompoland.com.

13. Sironi, A. et al. 2019. *Glossary on Migration. International Migration Law*. International Organization for Migration.

14. Tantaruna, L. 2019. "What is a migration crisis and how to address it integrally". *IOM*, August 30, 2019. https://rosanjose.iom.int.

15. UNHCR. 2022. "Registered Syrian Refugees in Host Countries". *UNHCR*, February 2022. https://www.3rpsyriacrisis.org.

16. UNHCR. 2022. "Operational Data Portal: Ukraine Refugee Situation". *UNHCR*, August 30, 2022. https://data.unhcr.org.

17. Wilson Center. (2019). "Timeline: the Rise, Spread, and Fall of the Islamic State". *Wilson Center*, https://www.wilsoncenter.org.

Jasmin Ahić*)
Kenan Hodžić**)

UDC: 341.311(470+571:477):355.45(497.6)
323.173(497.6)

THE WAR IN UKRAINE AND CHALLENGES FOR THE NATIONAL SECURITY OF BOSNIA AND HERZEGOVINA

Abstract: *The focus on international, regional and national security changed with the Russian invasion on Ukraine, and the geopolitical landscape dramatically put back on the agenda the instability in B&H, which could possibly have broader regional implications. The inspiration for exploring this phenomenon was originally related to the security situation of Bosnia and Herzegovina as a case study. A special aspect of the paper is the analysis of secessionism as a threat to national security, where we will draw parallels between the Ukrainian secessionism and Serbian secessionism. In order to accomplish this goal, we need to examine the threats that arise from the actions of political actors, speeches and discourses of the politics of secessionism in war and aggression. Some leaders manipulate the war records for political advantage; others are playing with the issues that caused the conflict and are still lingering.*

The scientific goal of this research is reflected in the description of international and national capacities, taking into account the structure of the political and security system, and the relations and connections between these systems. The social goal of this paper is to present findings about the secessionism as the main threat with serious potential, and to get acquainted with the key characteristics related to the responsibility of international security actors and risk factors.

The research is of a theoretical-empirical character. Given the interdisciplinarity of this research, to a greater or lesser extent, various general scientific methods will be used, primarily the hypothetical-deductive method and the analytical-deductive method, the method of scientific findings, and the method of analyzing the content of documents, events and testimonies in terms of analysis coordination and readiness of relevant actors in Bosnia and Herzegovina. In the amount of literature dealing with this issue, we will analyze relevant political discourse, scientific and professional papers, theoretical and empirical research, media sources in the form of reports and research, relevant legal legislation, but also the documents of international and other relevant organizations. This research should give this issue a more realistic dimension.

Key words: *Bosnia and Herzegovina, international security, national security, geopolitical conditions, secessionism.*

*) Full professor at Faculty of Criminal Justice, Criminology and Security Studies, University of Sarajevo.
**) Senior Assistant at Faculty of Criminal Justice, Criminology and Security Studies, University of Sarajevo.

INTRODUCTION

Perspectives on international, regional and national security have changed with the Russian invasion of Ukraine. The geopolitical landscape has once again put instability in Bosnia and Herzegovina on the agenda, which could have wider regional implications. The inspiration for researching this phenomenon is related to the security situation in Bosnia and Herzegovina. The paper is structured as a case study and will analyze the implications of the national security of Bosnia and Herzegovina due to the war in Ukraine. For conceptualization, a defining framework is important, where national security is viewed at the state level, within which the security of the nation that supports the state and the security of the state that responds and protects the national values and interests are combined (Bilandžić 2019, 280).

Bosnia and Herzegovina is poorly prepared for dealing with internal and external crises and represents a fertile ground for geopolitical battles between Russia and the West. As an internationally recognized state, Bosni and Herzegovina has been turned into a dysfunctional and divided state. Entity arrangement is dysfunctional because it enables blocking of state institutions, irrational because four levels of government make a huge, unprofitable and dysfunctional administration, undemocratic because it violates the fundamental human rights and discriminates against citizens of the state. The war in Ukraine reminded us how fragile is the current *status quo* in Bosnia and Herzegovina. Worsening of the security situation at the international level could potentially lead to more serious instability in B&H. The initial research question is whether the security situation in Bosnia and Herzegovina could be seriously undermined, but also whether the international security mechanisms are sufficient.

It is clear that aggression against Ukraine reflects the Russian state expansionism. Menkiszak (2014) points out that Putin's doctrine represents a conceptual plan for the Russian domination. That is why we will talk about the imperial aspirations of Russia and the attempt to create new rules for the whole world, and how this is reflected in Bosnia and Herzegovina. This paper tries to respond to the meaning and consolidation of the influence of the Russian Federation in Bosnia and Herzegovina, with reference to the danger of separatism. Therefore, the analysis in the paper will answer whether Russian ties with the leadership of the Bosnian-Herzegovinian entity Republika Srpska represent a significant problem in the conduct of state policy and whether there is actually a political-security synergy.

1. WHY IS THE WAR IN UKRAINE IMPORTANT FOR B&H?

With the invasion of Ukraine, there is a risk that Russia will use the existing tensions in the Western Balkans to destabilize the region. This applies not only to the north of Kosovo*), but also to Bosnia and Herzegovina as well, where leading Bosnian Serb politicians are threatening with secession of the Republika Srpska entity. Lachert, like many other analysts, states that diverting attention from Ukraine is a clear goal (Global 2022). He believes that the conflict between Serbia and Kosovo*) and the fragile political situation in Bosnia and Herzegovina are suitable for the Kremlin to destabilize the Western Balkans region. With a long list of unresolved internal affairs, conflicting political goals and security uncertainties, B&H possesses a worryingly large number of possible "triggers" for violence (Azinović, Bassuener, Weber 2012, 184). NATO's intervention in the Balkans in the 1990s – first in Bosnia and later against Serbia during the "Kosovo war" – has long been viewed by the Kremlin as a humiliating provocation. Since then, Russia has been increasing its influence and consolidating its position through separatist sentiments. In a 2017 study, Bechev stated that, when it comes to Bosnia and Herzegovina, Russian influence mainly refers to supporting separatism in the country and blocking B&H's access to the NATO alliance and blocking integration into the European Union. The International Crisis Group (2022) emphasizes that the secessionist movement threatens to break Bosnia and Herzegovina apart, while Kosovo* and Serbia, still remain at loggerheads over the former's status. Until these disputes are addressed, they will threaten regional stability. The war in Ukraine has a significant spillover effect into the Balkans, exacerbating existing divisions, highlighting the different geopolitical positions of countries in the region, and reigniting long-standing tensions between pro-Russian and pro-Western factions in the region (Giantin 2022).

*) UN Resolution 1244.

The research of the Center for Preventive Action, conducted in 2022, includes new unforeseen situations regarding the ongoing and potential conflicts (Stares 2022). Bosnia and Herzegovina found its place on this list. New contingencies consist of growing political unrest and separatist threats in Bosnia and Herzegovina. The Russians support the Serbs and the maximum autonomy for Republika Srpska, as well as wish to ensure that Bosnia never tries to enter NATO. Furthermore, it is not surprising that Russia refuses to recognize the authority of the Office of the High Representative in B&H and has announced its opposition to renewing the mandate of EUFOR in November 2021. Political leaders in the Republika Srpska have also refused to recognize the legitimacy of the High Representative and prevented it from addressing the RS Parliamentary Assembly (Szczerba, 2022). Miranova and Zawadewicz (2018), as well as Bajrović, Kraemer and Suljagić (2018) find that Moscow is arming and training Republika Srpska's police far beyond the levels required to deal with the normal law-and-order problems arising in the entity.

By supporting the increased militarization of Republika Srpska, Russia seeks to establish a client state where it can damage EUFOR peacekeeping mission Althea's credibility and weaken the transatlantic alliance. If destabilized, Bosnia and Herzegovina will be prevented from seeking further integration with the West. This can be seen as part of Russia's larger strategy to disrupt and reshape the international order. It is important to note that NATO and other major Western institutions deny membership to countries with undefined borders. Russia's support of efforts to divide and destabilize Bosnia thus serves to prevent its incorporation into these institutions (Hartwell, Karčić, and Mintel 2022). In terms of war in Ukraine, the parliament of entity Republika Srpska passed a set of conclusions in June 2022, one of them reaffirming a neutral stance on what was called "the Russia-Ukraine conflict" and another one on rejecting sanctions against Russia. While Bosnian and Croat leaders in Bosnia have condemned Russia's invasion of Ukraine, Bosnian Serb leaders have continued to seek closer ties with Moscow (Ernst 2022).

Milorad Dodik, the main Bosnian Serb leader, appeared at a public event with the Russian ambassador to B&H as a sign of support of Russia's aggression and has visited Moscow twice in 2022 in order to speak with the President of Russia Vladimir Putin and the Minister of Foreign Affairs Sergei Lavrov. The last visit coincided with Russia's announcement of a partial mobilization. Dodik has stoutly resisted B&H participation in sanctions against Russia. Until February 24, both the Kremlin and Milorad Dodik opposed the European Union's mission in Bosnia and Herzegovina and sought to eliminate or reduce it. However, after meeting with Vladimir Putin in June 2022 in St. Petersburg, Dodik claimed that Russia would approve the extension of the mandate if the further expansion of Operation Althea's troops is prohibited. The Kremlin and its allies in the Republika Srpska potentially perceive Althea as much weaker than NATO (Hartwell, Karčić, and Mintel 2022).

One MP from Dodik's SNSD party, Dušanka Majkić, threatened with a Russian military intervention should Bosnia and Herzegovina join NATO. Russia has added fuel to the fire by refusing to recognize the authority of the current High Representative in B&H and ended its financial support to the office. Also, Krastev (2022) points out that the national military of B&H needs to be modernized, but the budget has been blocked due to the political stand-off. This not only undermines the country's security, but also imperils the efforts of those in the country who want to align B&H more closely with NATO. It is now nearly impossible to engage in long-term defense planning due to this budgetary uncertainty. Dodik and his party may initially have seen in Putin's decision to invade Ukraine an opportunity to advance their goal of breaking up Bosnia and Herzegovina, because Dodik is also aware that the international focus on Ukraine could give him as well some space to unwind the current *status quo* in the Balkans. Dodik has been ready and willing to act as Moscow's agent, in return for political and financial support. Serwer warns that pattern – this a minority population that

constitutes a majority on particular territory calling on its "mother" country for protection and conducting a referendum on secession – is a classic irredentist technique that we have been seeing in Ukraine. Republika Srpska might join the Russian vassals in Georgia (South Ossetia[26)] and Abkhazia), Moldova (Transnistria), and Ukraine (Crimea, Donetsk, and Luhansk) as thorns in the paws of the West that distract the respective suzerains from pursuing membership in NATO and the EU (Serwer 2019, 60). Putin's invasion encouraged the nationalist leader Dodik from the Republika Srpska entity and President Aleksandar Vučić from the Republic of Serbia. In an interview given in June 2022, the Russian ambassador to Serbia, Aleksandr Bocan-Harchenko, noted that Republika Srpska remains one of the most important foreign policy goals of the Russian Federation, regardless of all the problems that the Russian state is currently facing (Srna 2022). Nutall (2022) explains that the Russian invasion of Ukraine adds fuel to the existing tensions in the Balkans. Moscow's propaganda spread throughout the Balkans by Russian media is fueling the fire as the war fuels the pro-Serbian rhetoric and heightens tensions across the region.

1.1. RUSSIAN PROPAGANDA AND MEDIA PATRONAGE

Russian propaganda has achieved the mobilizing power. Serbian media shows a high degree of empathy for Russians and compares Serbian suffering with Russian suffering, completely ignoring the crimes against the Ukrainian citizens (Atlantska inicijativa 2022). The Serbian media are part of the Russian propaganda machinery that creates an anti-Western atmosphere that further distances Serbia from European integration. The majority of public opinion is on the Russian side when it comes to the Ukrainian war. In the document entitled "Risks and Vulnerabilities in the Western Balkans", published by the NATO Center for

[26)] Since 2018, South Ossetia and Republika Srpska have signed an agreement on cooperation and friendship.

Strategic Communications (2020), it is emphasized that the insufficient level of cooperation and interoperability in the country is a major obstacle to the development of Bosnia and Herzegovina. In terms of national resilience, B&H is poorly prepared for dealing with internal and external crises. Special emphasis was placed on the lack of cohesion among the political elite regarding the country's foreign policy orientation, dysfunctional coordination in the event of a crisis, but also on the lack of awareness of the danger of information warfare and the ineffectiveness of state measures against hybrid threats. In 2016, the EU recognized and warned about Russian disinformation and propaganda warfare because Russia has the capacity and intention to conduct operations aimed at destabilizing other countries (European Parliament 2016). This often takes the form of support to political extremists and large-scale disinformation and mass media campaigns. The role of the media and the Russian state agency "Sputnik" is reflected in the effort to strengthen as much as possible the Russia's role as an arbiter in favor of Belgrade by fueling regional national conflicts, and therefore it is no coincidence that Serbs in Serbia, Bosnia and Herzegovina and Montenegro are considered as Russia's closest allies in the southeast Europe in a geopolitical struggle with the USA and Europe (Brey 2018).

Although most of the sources of political disinformation in BiH to be found among the local media, a large disinformation hub is formed by an alarmingly high number of media from neighboring countries, potentially used by foreign political actors. The Serbian edition of "Sputnik" is the only foreign-owned media in this hub. "Sputnik" is the only media with a presence in this hub which is owned by a state actor outside of the region, embodied in its Serbian-language outlet "Sputnik Srbija". The outlet also offers its radio broadcasts in the local language to several radio stations from both Serbia and B&H, and has a significant corpus of followers on social media. They found that "Sputnik" articles about B&H have a clear editorial bias towards the ruling party in the Republika Srpska, the Serb-led entity

in Bosnia and Herzegovina (AP 2019). This analysis showed that "Sputnik" has *de facto* acted as Dodik's campaign outlet prior to 2018 elections. Several EU countries, as well as NATO, were presented in these narratives as a threat to the Serbs, Republika Srpska, or Milorad Dodik in particular. His opponents were labelled as "puppets" of foreign actors and/or implicated in several conspiracy theories about the alleged coup plans or "colored revolutions" planned by the EU or NATO states. Milorad Dodik is undoubtedly the most prominent exponent of Moscow, but also the most invisible actor in Bosnia and Herzegovina. In this sense, he is also a potential generator of violent conflict (Biserko 2022). Serbia, as a key Russian partner, ensures Russia's survival in the region and expansion of its regional influence. In the political-security synergy of these two countries, the so-called construct of the Serbian world was created, which strongly relies on the Russian concept of the Russian World foundation. After the Montenegrin parliamentary elections in 2020 and the entry into power of open promoters of Russian interests, this construct was presented in Montenegro as well, through numerous high-level political and church addresses regarding Montenegro, Republika Srpska and Serbia. Šuklinov (2022) is of the opinion that the idea of a "Serbian world" begins in the Republika Srpska and Montenegro, where in 2016 the intelligence officers of the Russian GRU and Serbian rightists attempted a coup d'état. The "Serbian world" project is active, but it is dependent on Russia. There was even a Russification of Serbian nationalism (Politički.ba 2022). The identification of Orthodoxy with the Serbian, that is, the Russian Orthodox Church and Putin as the protector of all Orthodox Christians, represents a significant success of the Russian soft power in Bosnia and Herzegovina and its entity Republika Srpska, Serbia and Montenegro. We see from these examples that we are talking about narratives that justify the imperial ambitions of both Russia and Serbia. The "Russian World", as well as the "Serbian World", represent two irredentist projects similar in methodology. The first is oriented towards the return

of Russia as a global power, and the second towards the unification of Serbian territories (Atlantska inicijativa 2022). Halilović (2022) believes that the Russian doctrine and ideology of the Russian world, the doctrine and ideology of the Serbian world, the Croatian world and every other doctrinal and ideological large-state national world, are almost completely identical in content. It is only about variations of a general, common doctrine and ideology that differ from each other only by the name of the nation-state whose ethnocentrism is in question. Although presented as a project to protect the interests of the Serbian people in the region, this anachronistic modification of the idea of Greater Serbia in a very short period stirred up Montenegrin and Bosnian-Herzegovinian society and initiated a series of negative trends that already have an impact on the dynamics of the European integration of Montenegro and Bosnia and Herzegovina, with increasingly serious security implications (Digital Forensic Center 2021, 79).

2. NATIONAL SECURITY OF B&H AND IMPLICATIONS FOR INTERNATIONAL SECURITY

Indeed, the war in Ukraine has shifted the region's diplomatic dynamics. At a press conference following the Russia's invasion of Ukraine, NATO Secretary General Jens Stoltenberg stated the following: "The Kremlin is trying to make NATO and the EU provide less support to our partners. Our collective answer must therefore be more support to countries like Georgia, Moldova and Bosnia and Herzegovina. To help them succeed with their democratic reforms and pursue the path that they have freely chosen" (NATO, 2022).

Today, with growing poverty, fresh wounds from the pandemic, and the emerging tectonic geopolitical shifts that started on February 24, tensions in the region are probably at their highest level since the end of the last war. In B&H, the internal politics is currently divided between two administrative entities

(Federation of Bosnia and Herzegovina and Republika Srpska), on the one hand, and between three communities (Bosniaks, Serbs, Croats), on the other, each with different sources of certain external support. Just prior to the war, the EU's foreign policy chief, Josep Borrell, announced that the size of the EU's EUFOR Althea peacekeeping forces in the country would jump from 600 to 1,100 troops − a significant increase, although perhaps not sufficient to contain a consequential outbreak of violence, should one occur. The EUFOR characterized the deployment of these forces as a precautionary measure to strengthen the stability in B&H by positioning sufficient, capable forces to support the B&H government efforts to maintain a safe and secure environment. The signal was nonetheless clear and the mission has been to demonstrate the EU's determination to maintain stability in Bosnia and Herzegovina and to express its unequivocal commitment to the territorial integrity and sovereignty of the country (Shannon, 2022). The purpose of the increase in the presence of the international power is provision of more effective support to the state of Bosnia and Herzegovina and ensuring a safe and stable situation. The deployment of these forces is a precautionary measure, but the dilemma remains regarding the ability to credibly deter violence.

For almost a decade after the end of the war in 1995, NATO had the primary responsibility for peacekeeping in Bosnia and Herzegovina. In December 2004, the United Nations, in accordance with the Dayton Peace Agreement, adopted a resolution to establish a multinational military implementation force in Bosnia and Herzegovina. It is important to note that, through the Berlin Plus Agreements, Althea can draw on NATO troops, but this mechanism requires a decisive action from the European force. Consequently, NATO transferred its mission to Operation Althea. One key difference between Operation Althea and NATO is that, under Annex 1-A, Article I (a) of the Dayton Peace Agreement, Althea's mission must be approved by the United Nations. This means that all members of the UN Security Council, including Russia and China, must annually agree to

continue its mandate. The NATO's ability to act as the peacekeeping force in Bosnia and Herzegovina is authorized under a different section of the Dayton Peace Agreement. Annex1-A, Article I (b) states, "NATO may establish a force … under the authority of the North Atlantic Council." This permission is granted without a time limit or dependency on the UN Security Council approval. The fact that NATO transferred its peacekeeping mission to the European Union in 2004 does not affect the NATO's ability to reassume its previous role today. This means that NATO could legally deploy troops to Bosnia and Herzegovina, without acquiring permission from anyone, including the UN Security Council and the political leaders of Republika Srpska. The Althea's troop strength has varied. Originally, it was around 6,500 strong but dwindled over time to a mere 600 before invasion of Ukraine (Hartwell, Karčić, and Mintel 2022). The EU is working to stabilize the situation in B&H through its EUFOR Althea mission, and recently increased its military presence in that country in response to the mounting tensions and potential spill-over from the war in Ukraine. It derives its mandate from the United Nations Security Council Resolutions (UNSCR) 1551 and 1575. It provides deterrence and helps ensure the continued compliance with the terms of the Dayton/Paris Peace Agreement. By extension, it seeks to contribute to a safe and secure environment in Bosnia and Herzegovina in line with its mandate, the implementation plan of the Office of the High Representative (OHR) and the Stabilization and Association Process (EUFOR, 2021).

In 2021, the appointment of Christian Schmidt as the High Representative in Bosnia and Herzegovina was not confirmed due to opposition by Russia and China. Instead, Russia and China voted in favor of a resolution to end the mandate of the High Representative entirely. Although this resolution was not adopted, no UN Security Council resolution was proposed to confirm Schmidt as a result. All members of the Peace Implementation Council approved Christian Schmidt's appointment except Russia. The council's steering board does not require

unanimity for such a decision: Thus, Schmidt assumed the position of High Representative on August 1, 2021. The United Nations Security Council in November 2022 has renewed the mission of Operation Althea as the Bosnian peacekeeping force for one more year. This decision is positive in the short term, but the possibility of a Russian or Chinese veto is still worrisome in the long term. In addition to other warning messages, the French representative said that politicians who call for the secession of Bosnia and Herzegovina cannot be tolerated and condemned the glorification of war crimes and the denial of genocide (Klix 2022b). It is evident that this kind of environment destabilizes the country in security, political, economic and social terms. Blockade of the state, weakening of institutions, carelessness and social insensitivity are an excellent framework for making the rule of law and democratic order impossible, and for preparing the disruption of the security situation.

3. SECESSIONISM AS A THREAT TO NATIONAL SECURITY

Secessionism[27)] has a serious threatening potential for the peace and stability of B&H, the region and Europe as well. The problem is particularly acute in Bosnia and Herzegovina (B&H) where the government of the entity largely inhabited by Serbs, Republika Srpska (RS), is now actively seeking to break out of the state structures that have held that country together since the signing of the Dayton Peace Agreement. Threats arise from the actions of political actors, speeches and discourses of the politics of secessionism. Savanović et al. (2020) point out that secessionist rhetoric has been constantly present in the RS since the

[27)] When the domestic and international public talks about secessionism in Bosnia and Herzegovina, they mean first of all the possibility that the Republika Srpska, under certain conditions, in the foreseeable future, will call a referendum on independence on its own territory, which is an unconstitutional category and the scenario for the destruction of the Dayton Peace Accords, a new armed conflict and wider instability.

very beginning of its existence. In the period from 2006 to 2018, it has strongly intensified. The topic of secession did not appear in earlier OHR reports until 2006. It is important to note that arguments of illegitimacy, discrimination, inefficiency, "weak states", as well as arguments pointing to the factual situation and the right of the people to self-determination, are more often used in the discourse of political actors, in analogy with other secessionist movements in Europe. For years, the narrative of the political structures in the Republika Srpska entity has been reduced to the fact that Bosnia and Herzegovina, as a state, is regressive and unsustainable, and that its disintegration is imminent.

The key difference in previous actions is reflected in the fact that, at the end of 2021, when preparations for a military invasion of Ukraine were underway, the National Assembly of the Republika Srpska entity passed a controversial resolution in a step towards secession, raising tensions and provoking international condemnation. Despite the warnings of the international community and the boycott of the opposition, 49 of the 83 deputies of the National Assembly of the Republika Srpska (RS) adopted, on December 10, a resolution - supported by the leader of the Bosnian Serb Presidency at the state level Milorad Dodik, nowadays a President of the RS, as well as by the President of the RS Željka Cvijanović, the current Serb member of the Presidency of Bosnia and Herzegovina since the October 2022 elections – on the withdrawal from the army, service security, tax system and judiciary. The decision implies the transfer of authority from central institutions and leaves a six-month deadline for drafting new laws on the armed forces, the judiciary and the tax system. Some Western governments – namely Germany, the UK, the US, France, Italy – and the EU labeled, the resolution a "further escalation step" and threatened with introduction of new sanctions; the German Foreign Minister Annalena Baerbock called on the EU to impose sanctions on Dodik on December 13, but Dodik showed indifference and said that sanctions would lead them to their "true friends" (CrisisWatch 2022). The United

States and the United Kingdom imposed sanctions on various Bosnian politicians who are threatening the country's territorial integrity and who are engaging in corrupt activities. The European Union threatened to impose sanctions but did not do so, primarily because of the opposition from several EU countries, including Hungary, Croatia, and Slovenia (Hartwell, Karčić, and Mintel 2022). The Declaration on the Constitutional Principles of the RS was also adopted, which obliges the institutions of the RS to draw up a constitution according to which Banja Luka would be the capital of the entity, and Pale, not far from Sarajevo, would be the capital. The Declaration specifies that "all laws imposed by the High Representative are unconstitutional". Previously, on October 20, the same body passed the law on medicines and medical devices, which provides for the establishment of an entity agency for medicines, operating at the state level since 2009. According to the Constitution of B&H, the entities cannot independently return the competences that were transferred to the state in the past period (Huskić 2021).

The essential international mechanism, The Peace Implementation Council, an international body set up to oversee the implementation of the 1995 Dayton Peace Accords, said on February 10 that the law establishing the entity's High Judicial and Prosecutorial Council would create an "unconstitutional body, which would threaten basic legal rights of all citizens of Bosnia and Herzegovina". On the same day, the American Embassy in Sarajevo announced that this move "will allow criminals to prosper and corruption to flourish" (CrisisWatch 2022). In response, the leader of the opposition Serbian Democratic Party, Mirko Šarović, described this move as a "direct threat to peace" that would lead RS "into a spiral of war".

The Peace Implementation Council is an international organization formed in 1995 to implement the Dayton Peace Agreement, and it has been operational in conjunction with the Office of the High Representative ever since. The Office of the High Representative has shifted the course of action throughout the previous 12 years. The High Representative Christian Schmidt's warning from the end of

2021 looms: "The prospects for further division and conflict in Bosnia and Herzegovina are very real". However, the OHR was not used by the Bonn authorities between 2011 and 2021, after which it was revived in April 2022, given the perceived severity of Serbian moves for secession. Since then, the incumbent High Representative Cristian Schmidt has intervened to block RS claims for state assets in April 2022, override HDZ's veto on fully funding the upcoming elections, impose an electoral "integrity package" in July, and amend the constitution FB&H in October 2022. The issue of state property is precisely the area of the new-old political crisis and radicalization of discourse. In November 2022, Dodik emphasized the following: "If someone dares to interfere in the property and legal relations of the RS without discussion and despite our idea of it, they will sign the decision that I will propose here on the secession of the Republika Srpska" (N1 Sarajevo 2022).

According to this review, we see that the continuity of secessionist statements shows that it is a matter of strategic orientation. Szczerba (2022) in his report to NATO states that, prior to the outbreak of war in Ukraine, the parliament of the Republika Srpska announced its intention to pull out of the federal tax, judicial and military systems and to establish their own instead. Powerful secessionist sentiments in Republika Srpska have led to a paralysis of government and budgetary gridlock. This blockage has impeded the country's democratic and economic development on a range of fronts. The constitutional order, set up in the Dayton Accords, cannot function without inter-communal cooperation, and this simply is not present today. Indeed, the Republika Srpska has embarked on an effort to construct parallel institutions which would lead to a *de facto* secession. The Croatian parties have also been obstructionist and are deeply dissatisfied with the current constitutional order. One of Dodik's unlikely allies is the Bosnian Croat leadership, particularly Dragan Čović, a former Croat member of the tripartite presidency and leader of the Croatian Democratic Union of Bosnia and

Herzegovina. Čović and Dodik often work in concert to further divide the country to consolidate their power and influence. Čović has echoed Dodik's divisive rhetoric and has argued for a third "Croatian" entity in the south of Bosnia and Herzegovina, another move that undermines Bosnian sovereignty (Hartwell, Karčić, and Mintel 2022). In the given (geo)political circumstances, Milorad Dodik will continue to suggest strategic patience, resistance, various types of obstructions, strengthening the combat readiness of the RS police, etc. Therefore, he will be patiently waiting for the unfolding of the (geo)political situation and an opportunity that will come if the external circumstances change in his favor (Klix 2022a). In the dark perspective, in the absence of collective security mechanisms, Milorad Dodik would have crossed the point of no return and fulfilled his repeatedly repeated promise - the declaration of the RS independence.

CONCLUDING REMARKS

Bosnia and Herzegovina, as a state, is a historically interwoven multiethnic community. The European crystal palace, built on the illusion of the end of history, eternal peace and the triumph of liberal democracy, can collapse at any moment, precisely in Bosnia and Herzegovina. From the signing of Dayton until today, this agreement has experienced a lot of criticism, and represents a field for political manipulations and contradictions. The war ended with the Dayton process in 1995, and none of the warring parties was fully satisfied with this agreement. The disputes were of a territorial, political, legal and symbolic nature.

However, it should not be overlooked that this project for peace represents the only possible model of peace and prosperity for B&H in the current international and internal circumstances. Over time, many international circumstances have changed, and so have the requirements for Dayton. The Ukrainian war is an extraordinary warning to all external entities to take B&H more seriously. The

Russian ties with the leadership of the Bosnian-Herzegovinian entity Republika Srpska trully represent a significant problem in the conduct of state policy, and the political-security synergy represents a danger in the current conditions and relations. Stabilizing Bosnia and Herzegovina is the most pressing need. The risk of conflict exists due to Russia's broader geopolitical interests and secessionist threats, despite a slight increase in EUFOR forces and the ongoing international diplomatic mediation efforts.

The coordinated destabilization of the region is visible, followed by media coverage. If the malignant idea of separating Republika Srpska from the state of Bosnia and Herzegovina succeeds, it would be a sign that the time has come for a new world geopolitical order, in which new state borders are drawn and new states are created under the patronage of Russia. The secessionism of the Republika Srpska entity is a political fiction, a mere propagandistic hoax and an artificial debate that the nationalist leader Milorad Dodik skillfully deconstructs into an alliance with the Kremlin.

The perspective and future of B&H lies in integrations and extensive reforms that will increase the well-being of the country and contribute to peace and stability, both within B&H and in the region. On the other hand, in response to the reawakened threat of security as a form of more organized violence, state power must be affirmed and strengthened in the sign of national security.

REFERENCES

1. Aktuelno. 2022. “Ruski propagandisti u velikom problemu: “Toksične” Propagandne Platforme Bliske Službama I Crkvi Srbije U Panici Od Gašenja!”. https://www.aktuelno.me.
2. AP. 2019. “How Serbian Sputnik Infiltrated a Disinformation Hub in Bosnia and Herzegovina.” EUvsDisinfo. June 14, 2019. https://euvsdisinfo.eu.
3. Atlantska inicijativa. 2022. “Proruska Propaganda U Srbiji.” Atlantskainicijativa. https://atlantskainicijativa.org.
4. Azinović, Vlado, Kurt Bassuener, and Bodo Weber. 2012. *Assessing the Potential for Renewed Ethnic Violence in Bosnia and Herzegovina: A Security Threat Assessment*. Sarajevo: Fakultet političkih nauka, Univerzitet u Sarajevu.
5. Bilandžić, Marko. 2019. *Nacionalna Sigurnost: Prognoziranje Ugroza*. Zagreb: Despot infinitus.
6. Biserko, Sonja. 2022. “Srpski Svet.” Gradski Portal. October 21, 2022. https://gradski.me.
7. Brey, Thomas. 2018. “Russian Media Power and Revisionism in Serbia.” *Südosteuropa Mitteilungen*, no. 04: 26–41.
8. CrisisWatch. 2022. “CrisisWatch Database.” Www.crisisgroup.org. August 30, 2022. https://www.crisisgroup.org.
9. Digital forensic centar. 2021. “DFC Studija - Uloga Rusije Na Balkanu: Slučaj Crne Gore – Dfcme.me.” Https://Dfcme.me/. September 16, 2021. https://dfcme.me.
10. Ernst, Iulian. 2022. “Bosnia’s Republika Srpska Seeks Stronger Economic Ties with Russia.” Intellinews.com. August 14, 2022. https://intellinews.com.

11. EUFOR. 2021. "European Union Force in BiH, Operational Althea". https://euforbih.org.

12. Evropski parlament. 2016. "Usvojeni Tekstovi - Strateška Komunikacija EU Za Borbu Protiv Propagande Koju Protiv Nje Provode Treće Strane – Srijeda, 23. Studenog 2016." https://www.europarl.europa.eu.

13. Giantin, Stefano. 2022. "Russian Aggression Isolates Serbia, Divides Bosnia, Unites the Rest of the Balkans." Nato Defense College Foundation. February 28, 2022. https://www.natofoundation.org.

14. Global, Bosna. 2022. "Warsaw Institute: Ruski Cilj – Tenzije Na Balkanu, Skretanje Pažnje Sa Ukrajine." Bosna Global. July 4, 2022. https://bosnaglobal.net.

15. Hartwell, Leon, Hikmet Karčić, and Josephine Mintel. 2022. "Send NATO Troops to Help Stabilize Bosnia and Herzegovina." War on the Rocks. August 12, 2022. https://warontherocks.com.

16. Huskić, Adnan. 2021. "Skupština Pokrenula Proces Prenosa Nadležnosti Sa BiH Na RS." Radio Slobodna Evropa. December 10, 2021. https://www.slobodnaevropa.org.

17. Klix. 2022a. "Hadžikadunić: Bez NATO-a BiH Bi Izgledala Kao Libija, Dodik Čeka Geopolitičku Priliku." Www.klix.ba. July 5, 2022. https://www.klix.ba.

18. Klix. 2022b. "Francuska O Stanju U BiH: Ne Mogu Se Tolerisati Lideri Koji Pozivaju Na Secesiju." Www.klix.ba. November 2, 2022. https://www.klix.ba.

19. Krastev, Ivan. 2022. We Are All Living in Vladimir Putin's World Now. The New York Times. https://www.nytimes.com.

20. Menkiszak, Marek. 2014. "The Putin Doctrine: The Formation of a Conceptual Framework for Russian Dominance in the Post-Soviet Area." http://www.osw.waw.pl.

21. Miranova, Vera and Bogdan Zawadewicz. 2018. Putin Is Building a Bosnian Paramilitary Force. Foreign Policy. https://foreignpolicy.com.

22. N1 Sarajevo. 2022. "Dodik: I Will Propose Secession If Anyone Interferes with RS Entity Property." N1. November 15, 2022. https://ba.n1info.com.

23. Nuttall, Clare. 2022. "Five Days to Preserve Peace in the Western Balkans | BALKAN BLOG." Www.intellinews.com. August 26, 2022. https://www.intellinews.com.

24. Politicki.ba. May 4, 2022. https://politicki.ba.

25. Reuf Bajrovic, Raichard Kraemer, and Emir Suljagic. 2018. Bosnia on the Russian Chopping Block: The Potential for Violence and Steps to Prevent It. Foreign Policy Research Institute, https://www.fpri.org.

26. Savanović, Aleksandar, Aleksandar Vranješ, Nevenko Vranješ, and Željko Budimir. 2020. "Izvori, Geneza I Priroda Secesionističke Retorike U Republici Srpskoj." *Politička Misao* 57 (1): 93–126. https://doi.org.

27. Serwer, Daniel Paul. 2019. *From War to Peace in the Balkans, the Middle East and Ukraine*. Cham, Switzerland: Palgrave Macmillan.

28. Shannon, Seamus. 2022. "EUFOR Reserve Activation 2022", EUFOR Operation ALTHEA. https://www.euforbih.org.

29. Srna. 2022. "Bocan Harčenko: Položaj Srpske Prioritet Spoljne Politike Rusije." Nezavisne Novine. June 16, 2022. https://www.nezavisne.com.

30. Stares, Paul B. 2022. *Preventive Priorities Survey*. *Council on Foreign Relations: Center for Preventive Action, New York*. New York: Council on Foreign Relations: Center for Preventive Action.

31. Szczerba, Michal. 2022. The Western Balkans: Russia's war on Ukraine and the region's enduring challenges, NATO Parliamentary Assembly, ESCTD.

Mitko Arnaudov*)

UDC: 314.151.3-054.72:323-044.372(497.7)
314.151.3-054.72:338.1(497.7)

MIGRATION IN THE 21ST CENTURY – DETERMINATOR OF POLITICAL, SECURITY AND ECONOMIC SUSTAINABILITY OF NORTH MACEDONIA

Abstract: *During the last two decades, North Macedonia has been facing the phenomena of huge emigration as a consequence of unstable political, security and economic flows in the country. Based on the results of the last census in that country, held in September 2021, this country lost more than two hundred thousand people in a period of twenty years, which, from a strategic point of view, represents a huge internal issue for the ongoing economic flows, potential economic growth and national investment strategies. Most of the emigrants have stated that the main reason for leaving the country were unstable economic perspectives, continuation of political tensions and politically initiated ethnic problems, which all contribute to security instability. Such circumstances are the reasons for emigrants to decide to start a new chapter in life abroad, mostly in the Western European countries. Moreover, long duration of the European integration of North Macedonia represents one of the key reasons why many young citizens of this state have decided to emigrate. In this paper, from a practical point of view, the author will analyze and explain the key reasons of the migration phenomena in North Macedonia, as well as how these reasons contribute to its economic, political and security sustainability on middle term. From the other side, from a theoretical point of view, we are going to explain how much small states, such as North Macedonia, without strong economic performances and political power on regional and international level, are vulnerable, from the perspective of migration, in contemporary globalized international relations. The questions we would like to reach an answer to in this paper are the following: Do small states, on the example of North Macedonia, could be sustainable if the process of globalization at the same time determines the process of migration? What mechanisms small states have in order to mitigate the migration flows, as a measure in securing economic sustainability? Does faster European integration contribute to mitigation of migration, or the contrary? How much do the political instability and security threats really contribute to emigration process?*

Key words: *Migration, Economy, Politics, Security, Sustainability, Integration, North Macedonia, European Union.*

*) Research Fellow, Centre for Neighboring and Mediterranean countries, Institute of International Politics and Economics.

INTRODUCTION

The problem of migration has been attracting the interest of the European and the world public for many years, but it came into the spotlight during the refugee crisis in 2015 and 2016. The large population movement, first from Asia and then from North Africa to the developed countries in Europe, has caused administrative, financial, and then political problems, both in the countries of transit and in the countries of final destination (Lutovac, 2018, 9). This issue has caused huge problems also in the Western Balkans region, primarily because of the already existing problems faced by these countries at the institutional level. At the same time, the migration problem, placed in the context of the European integration, has a particular importance for the research of the functioning of institutions and the process of operationalization of the European values, both in the EU and in the Western Balkans region, which is participating in the European integration process (Lutovac, 2018, 9). The Western Balkans geographic region – comprised of Albania, Bosnia and Herzegovina, Croatia, Kosovo*), North Macedonia, Montenegro, Serbia, and Slovenia – is no stranger to refugee flows, having experienced massive displacement as a result of violence and ethnic cleansing during the 1990s (Greider, 2017). When it comes to North Macedonia and the migrant crisis that gripped the European continent in 2015 and 2016, this country has blocked the border with Greece, with the intention of stopping the further arrival of refugees on its territory, but such decision of Macedonian authorities was in direct opposition to the proclaimed policy of Germany, which was based on an invitation to refugees to travel freely (Kuljić, 2018, 13). In fact, the migrant crisis presented multiple challenges to the European Union: first, political (review of the Schengen Agreement, determination of a common position and unified policy, reaction to Turkey's blackmail policy), economic (additional costs of care and allocation for Turkey), then cultural (integration of a million Muslims), and the comprehensive security challenge (the securitization of the migrant issue and the reconstruction of the common European security area) (Radinović, 2018, 276).

*) UN Resolution 1244.

The challenges of the migrant crisis have caused numerous problems in the region of the Western Balkans as well. Because the states of this region, even though they were not members of the European Union, at that moment were forced to guard the external borders of the Union, primarily taking into account the fact that the migrants did not want to stay in the territory of Greece, nor in the territory of the Western Balkans region. In the case of North Macedonia, migrant crisis saw the effects of deploying police forces from the member states of the European Union, but also from neighboring countries, such as the Serbian police forces, on the borderline between this country and Greece. The goal of these "mixed" police forces was to contribute as much as possible to the management of migrant flows, the prevention of illegal migration, and the prevention of human trafficking. The migrant pressure that North Macedonia faced during 2015 and 2016 was particularly strong, considering the country's limited institutional, economic and security capacities. In North Macedonia, an unrelated political crisis related to corruption scandals in that period meant that the migration flows did not receive as much media attention as in other countries. And if anything, the government's ability to close the border in that period and act on internationally brokered agreements shored up its legitimacy against the opposition party (Greider, 2017). During the peak of the European migration and refugee crisis, hundreds of thousands of asylum seekers and migrants arrived in the European Union via the Western Balkans. In 2015, 600,000 of refugees and migrants were registered in the Presevo camp alone, on the border of Serbia and the North Macedonia (Greider, 2017).

At the same time, during the last twenty years, North Macedonia has been facing the problem of internal emigration. A significant number of the population decided to leave the country due to poor living conditions, primarily low living standards, lack of jobs for qualified individuals, political clientelism, but also institutional inefficiency, which creates additional insecurity in the society of this country. When it comes to economic migrations or the so-called migrations of the working population, it is important to point out that they represent movements of

the population in search of work outside the borders of their country of origin and their roots can be found in the last quarter of the 19th century (Ljuboja, 2015). The trend of constant growth in the number of migrants from the Balkans is also confirmed by the data of the European Statistics Agency (EUROSTAT) (Vučković, 2022). Countries such as Serbia, Bosnia and Herzegovina, Albania and North Macedonia continue to show a high emigration character, even in spite of a significant drop in emigration at the beginning of the 21st century (Ljuboja, 2015). In North Macedonia, there are no official statistics on young people who have left the country in the past 10 years, but it is estimated that their number is not less than 200,000. These numbers testify to the danger of population loss in North Macedonia, which, in the medium term, brings into question the sustainability of this country, primarily in the economic context, due to the labor force deficit that increases year by year on the labor market in that country.

A Professor at the University of "Ss Cyril and Methodius" in Skopje, Ilija Aceski, said that polls show that a dysfunctional state and the inability to find employment legally, through a competition, are the top reasons why young people leave the country (Vučković, 2022). "The major problem is the fact that young people are losing or have already lost faith in public institutions and the state, and the worst thing is that young people in North Macedonia do not see perspective, at all" says Aceski (Vučković, 2022). Internal migrant challenges actually represent contemporary security challenges of countries because, in the medium and long term, due to the lack of qualified labor force, bring into question the sustainability of a country's system infrastructure. In North Macedonia, entire settlements are being emptied and left without inhabitants, and according to the results of the census, published at the beginning of 2022, this alarming situation is evident in certain parts of the country (Simovski, 2022). In the 2002 census, there were 147 settlements without inhabitants, while according to the latest census, that number increased to 207.

1. POLITICAL CRISIS AND ECONOMIC PERFORMANCE AS THE MAIN CAUSES OF EMIGRATION IN NORTH MACEDONIA

The Republic of North Macedonia has been facing a succession of political crises since the independence until today. The unstable internal political situation in that country greatly contributes to poor economic performance, and thus to the poor living conditions of the population, regardless of their national, ethnic or religious affiliation. Pervasive corruption in North Macedonia largely determines political trends and makes political institutions unstable, inefficient and ineffective. In fact, the Republic of North Macedonia has always been considered a highly intensive migration area, characterized by both exhaustive inner movements of its citizens, as well as continuous emigration processes towards other countries (Sotiroski, Hristoski, 2014, 33). North Macedonia has entered the new millennium with social problems, ethnic tensions and economic instability (Apostolovska-Toshevska, Madjevikj, Ljakoska, Gorin, Radevski, Dimitrovska, 2018, 59). Almost 2/3 of the emigration flows are directed towards some of the European countries (Germany, Switzerland, Italy and other), out of which 12.1% towards America and almost 10% towards Australia and Oceania (Apostolovska-Toshevska, Madjevikj, Ljakoska, Gorin, Radevski, Dimitrovska, 2018, 61). Apart from this trend of permanent emigration, many young people, mainly students, go to work abroad for a limited period of time through employment agencies or students' "work and travel" and "internship" programs. Most of them work in Germany, Italy, Austria, Sweden, the USA, Canada and Australia (Apostolovska-Toshevska, Madjevikj, Ljakoska, Gorin, Radevski, Dimitrovska, 2018, 62). Based on the Eurostat data (2014), in the European countries alone, the number of Macedonian citizens increased from 135,000 in 2000 to 240,000 in 2014.

"The largest increase is noticed in the receiving countries of the European Union, especially in 2011, after the stagnation during the economic and financial crisis (2008–2010) (Apostolovska-Toshevska, Madjevikj, Ljakoska, Gorin, Radevski, Dimitrovska, 2018, 63). In North Macedonia, the unsustainability of economic policy is actually the main cause of emigration. The strong influence of political subjects in the creation of economic policies contributes to an unfavorable economic situation that directly threatens the inhabitants of this country who reject the so-called clientelist model of ensuring economic sustainability.

In North Macedonia, the political elites are abusing the inter-ethnic relations, as well as political opponents as a mechanism for an additional division of the society on different levels, and in ,that way the politicians are succeeding in marginalizing the real economic problems within the country, as a leading reason for emigration. The fact that almost 452,000 people in North Macedonia in 2022 live below the poverty line, according to the latest data from the State Bureau of Statistics, represents a significant indicator of the large emigration of the country's population (Mitevska, 2022). The cost of living in April 2022 in North Macedonia was 10.5 percent higher compared to the same month last year, while retail prices were 11.1 percent higher in the same period. From the other side, the state debt reached a record level of over 7.1 billion euros, or more than 60 percent of the gross domestic product (GDP). "We can no longer talk about economic development, but economic survival. This implies that capital investments must continue in order to maintain the continuity of the private sector", says the economic analyst Arben Halili (Mitevska, 2022). The unstable political situation, the irresponsibility of the political elite, as well as the widespread corruption, determine the economic problems in North Macedonia, which directly result in a significant number of the population leaving the country.

The great indifference and inferiority of the youth, especially students, who should be the generators and the critical mass of the society, is evident in North

Macedonia. The latest research detects an increasing mass exodus of young people, especially intellectuals from North Macedonia, who are most often looking for a "better tomorrow" in the Western Europe countries. This trend of "brain drain" is becoming more and more worrying and it is the topic of many formal and informal youth meetings (Fazlagić, 2013). Hundreds of thousands of Macedonians have already left the country. According to the World Bank statistics, a half a million of Macedonians already live abroad. That is about a quarter of the total population. One of the Macedonians who already lives and works abroad says that a good job in North Macedonia requires political connections (Deutsche Welles, 2020). Such tendencies bring into question the sustainability of North Macedonia because of three key reasons: first, this country is continuously losing its working-age population; second, the decreasing number of working-age population makes the national pension system unsustainable; an third, the country is becoming less and less attractive for new investments as a consequence of the deficit in the labor market.

The large variations in the official statistics for 2012 and 2013 between the OSCE and the State Bureau of Statistics of North Macedonia testify to the fact that North Macedonia does not lead a serious policy, even when it comes to migration flows. Thus, according to the data of the State Statistics of North Macedonia, in 2012, 1,330 inhabitants emigrated from that country, while in 2013, only 945. On the other hand, according to official OSCE data, 17,530 inhabitants emigrated from North Macedonia in 2012, while in 2013, as many as 20,562 of them did the same (Vračić, 2018). In the countries of the region, there are no exact statistical data on the number of young people who have permanently emigrated since the beginning of the new millennium, and all estimates are based on the OSCE database for the period from 2012 to 2016. During that period, an average of slightly more than 9,500 of mostly young people left North Macedonia annually (Radio Slobodna Evropa/CDM, 2022).

The poor living conditions of young people in North Macedonia is evidenced also by the fact that an increasing number of them want to continue their lives abroad. According to the latest research, 58 percent of young people say that they would move out of the country, and 64.8 percent are dissatisfied with their place in the country. According to the research of the Foundation for Democracy in Westminster, in North Macedonia, there is a high degree of youth dissatisfaction related the fact how state authorities take care of this category of people, and there is a huge discrepancy between the opportunities and needs of young people at the local level and at the central level (Deutsche Welle, 2022). Many young people decide to move because of the opportunities they have in other countries in terms of social life, cultural events, educational opportunities, etc. Therefore, the reasoning is that in these areas the state (North Macedonia) should try to find solutions[28)] that will attract young people to stay in their country. The most common emigration is present among the highly educated staff from the field of medical professions, as well as from the field of engineering, who have gone to the EU member states in recent years, and especially to Scandinavia, Germany, Britain (Deutsche Welle, 2022). Better work conditions and economic perspectives are not the only reasons for young people to leave North Macedonia. The trends of leaving in recent years have also been attributed to the non-economic reasons – they are bothered by pollution, politics, corruption, and in an open world, in which there are no barriers to migration, young people leave easily, without hesitation. Although North Macedonia has a National Strategy for cooperation and preventing the brain-drain of young and high-quality personnel 2013-2020, it was not implemented, which is shown in the analysis of the Brain Drain Prevention Network – composed of seven civil society organizations working in various areas related to development of young people, youth policies and rights and youth

[28)] Aiming to stop the negative migration trends in North Macedonia, the authorities have adopted the Government Program 2022-2024, which provides support for each employed person up to the age of 29 who will be employed for the first time, for all those who have not yet developed employment skills to do so through practice. A personal income tax refund is provided for all newly employed young people under 30 years of age; the support is also seen in the opening of youth centers and local youth councils, with the aim of involving young people in decision-making processes and increasing the capacities of the youth.

information (Večer, 2020). According to the World Bank data, in the last ten years, half a million citizens have emigrated from North Macedonia, most of whom are young. The research conducted by the German foundation "Friedrich Ebert", with participation of 1,200 respondents, shows that only eight percent of young population wants to stay in North Macedonia, while two thirds of young people want to emigrate (Večer, 2020). These trends undoubtedly further bring into question the overall sustainability of North Macedonia. Emigration of young people not only affects the reduction of the population in the medium term, but also makes the institutional infrastructure of the country non-functional because the number of employees who retire will not be replaced by new personnel over time due to the increasingly pronounced labor force deficit on the labor market.

2. MODERN SECURITY CHALLENGES AS A NEW GENERATOR OF EMIGRATION IN NORTH MACEDONIA

The security challenges faced by the North Macedonia from 1990 to 2010 were not the cause of increase of the rate of emigration among the population of this country during the mentioned period. More precisely, the wars in the territories of the former Yugoslavia during the nineties, as well as the economic sanctions that this country was faced with immediately after the declaration of independence, did not affect the residents moving out in large numbers. The largest migration of the Macedonian population was recorded in 2001, during the armed conflict in the north-western parts of the country. But, in this case, it is primarily about the internal migration of the population, that is, on the territory of North Macedonia. According to the Ministry of Labor and Social Policy, during the eight months of the conflict, there were over 140,000 displaced persons in North Macedonia (Popovski, Naumova, 17). But, the important thing in the context of armed conflict and migration, what is important is the data that in the year after the conflict ended: approximately 90% of the population gradually returned to their homes (Popovski, Naumova, 18).

On the other hand, North Macedonia continuously began to face population emigration due to the unwillingness of the national system to face with the modern security challenges that are not related to the so-called traditional threats of sovereign states, such as the threats to political sovereignty and territorial integrity. In that context, as Gocevski and Gjurovski have stated, the theories of security and peace unequivocally indicate that one of the key factors for the promotion and preservation of world peace is precisely raising the level of economic development of countries (Gocevski, Gjurovski, 2017 pp.20. op.cit.). North Macedonia is nowadays facing security threats such as economic underdevelopment, weak and dysfunctional institutions, as well as a health system that does not respond to modern challenges in the field of public health. These challenges create intra-institutional security challenges, respectively, the institutional infrastructure of North Macedonia creates contemporary security threats which directly threaten the security of citizens in the context of creating conditions for normal life. Based on it, as we have mentioned previously in this paper, numerous young citizens of North Macedonia are deciding to emigrate because they are not satisfied with the living conditions that public system in this country provides them.

The best modern example in that context is the health system of North Macedonia facing the *Covid-19* pandemic. During the *Covid-19* pandemic, the North Macedonia has applied more or less the same measures as its neighboring countries. Basically, all of them applied "copy-paste" measures in the fight against *Covid-19*, but North Macedonia fared the worst, because it has had the largest number of new *Covid-19* cases and deaths in relation the number of citizens. The difference between North Macedonia and other neighboring states was only in the measures for entering and leaving the country, where state quarantine was obligatory for Macedonian citizens, as well as for foreigners (Mirilović, 2022). During the *Covid-19* pandemic, the citizens of North Macedonia were faced with numerous systemic inconsistencies, which have led to a sudden increase in the number of infected people, but also to a high mortality rate due to the inconsistency and inefficiency of the national health system.

Even the NATO membership of North Macedonia did not enable provision of better conditions for overcoming the contemporary security threats faced by the North Macedonia's citizens. Although NATO allies through the Euro-Atlantic Disaster Response Coordination Centre (EADRCC) have provided different types of assistance to North Macedonia in the fight during the *Covid-19* pandemic, internal institutional and systematic problems in this country were a crucial reason for such negative trends during the pandemic. According to data from September 1, 2022, North Macedonia, from the beginning of the *Covid-19* pandemic, has registered 340,510 cases, from which 329,434 recovered patients and 9,490 deaths, which position this country in the group of the list of European countries with the highest rate of mortality due to the pandemic (Worldometers, 2022).

In fact, modern security challenges, such as political instability, the unsustainability of the health system and weak economic development are the key determinants of the emigration of the Macedonian population, which, as a process determined by internal problems, is also a security challenge in itself, because it contributes to further reducing the capacities for creating long-term sustainability of North Macedonia.

CONCLUSION

Migration flows are a modern trend present in all parts of the globalized world. In fact, the process of globalization has directly contributed to the promotion of a large-scale migration due to the ever-increasing possibilities of population movement. The great mobility of the population on the global level was generated by economic processes and trade exchange at all levels, but also by modern technologies that significantly influenced the simplification of mobility of the world's population. There are different reasons for world population migration. If only a hundred years ago the reason for migration were the struggle for fertile

land and food production or to avoid wars, today it is primarily due to economic reasons, i. e. the wish to ensure better living conditions, not just basic human needs, such as food and water. But we should not ignore the fact that wars have remained one of the main reasons for migration, which we saw in the example of civil wars in the former Yugoslavia, but also in the example of war conflicts in the Middle East, North Africa and the ongoing war in Ukraine. Almost millions of people were displaced as a consequence of the armed conflicts in the Middle East and north of Africa which, in fact, were the cause of the European migrant crisis during 2015 and 2016.

On the other hand, when we talk about the migration of the young population, the main reasons for migration are primarily the living conditions, respectively, finding better economic conditions, as well as the stable systemic organization of a society. Based on the existing data, it can be reiterated that the main causes of increased population migration in North Macedonia are poor living conditions that appeared as a consequence of systemic inefficiency and ineffectiveness. In fact, in North Macedonia, it is a cause-and-effect process that is continuously contributing to the collapse of the sustainability of this country. At the top is an inefficient and dysfunctional political system, riddled with continuous political crises and corruption scandals. Such a political system contributes to the constant collapse of the infrastructure of the public system in the economic, health, educational, security and social contexts. So, the collapsed infrastructure of the public system of North Macedonia is enabled to perform its basic function, respectively, to serve the citizens. On the other hand, such a dysfunctional public system not only does not serve the citizens, but additionally threatens their safety, which is most clearly presented in the way of responding during the *Covid-19* pandemic. All this contributes to the increase of the emigration of the Macedonian population, which is not only a consequence, but also a new-established problem that additionally determines the political, economic and security trends in this country in a negative

way. The emigration of the population of North Macedonia, especially young and educated population, is a pervasive problem of this country, which in the medium and long term, affects not only the overcoming of existing systemic problems, but also the creation of new challenges that permanently block all potentials for the development of this country. The development of the economic system is almost impossible, due to the deficit of qualified labor on the labor market, which automatically deters potential new investments. The social and pension system became dependent on foreign lending, due to the impossibility of creating new additional value, so in that context, the public expenditures are based on external credit institutions. At the same time, the education system becomes absolutely dysfunctional because it produces new qualified workforce who are placed on foreign markets; at the same time, there is no return of value from investing in qualified workforce through the public education model. In fact, all this leads to conclusion that emigration is the main problem and challenge for North Macedonia, which as a process should be stopped, so that another process of solving the systemic and all-pervasive institutional challenges should start, which as a consequence of its functioning has produced migration.

REFERENCES

1. Vračić, Alida. 2018. “Put za povratak: Odlazak obrazovanih ljudi i prosperitet na zapadnom Balkanu”. European Council on Foreign Relations. https://ecfr.eu.
2. Večer. 2020. “Младите сакаат да се иселат, причините не се само парите”. https://www.vecer.press.
3. Vučković, Branko. 2022. “'Mladi odlaze trajno': Migracije sa Zapadnog Balkana”. Radio Slobodna Evropa. https://www.slobodnaevropa.org.
4. Greider, Alice. 2017. *Outsourcing Migration Management: The Role of the Western Balkans in the European Refugee Crisis*. Brussels/Washington: Migration Policy Institute.
5. Deutsche Welle. 2020. “Zemlje bez mozgova, zemlje bez budućnosti”. https://www.dw.com.
6. Deutsche Welle. 2022. “Истражување: Од младите 58 проценти би се иселиле”. https://www.dw.com.
7. Kosovo Online/Telegrafi. 2022. “Simovski: U Severnoj Makedoniji za 20 godina oko 10 odsto manje stanovništva”. https://www.kosovo-online.com.
8. Kuljić, Đorđe, 2018. “Odgovor Srbije na izbegličku krizu u kontekstu puta ka članstvu u EU”. U: *Savremene migracije i društveni razvoj: interdisciplinarna perspektiva.* Tematski zbornik vodećeg nacionalnog značaja 2018. Beograd: Srpsko sociološko društvo, Institut društvenih nauka, Univerzitet u Beogradu, Filozofski fakultet, Institut za sociološka istraživanja.
9. Lutovac, Zoran. 2018, “Reč urednika”. U: *Savremene migracije i društveni razvoj: interdisciplinarna perspektiva.* Tematski zbornik vodećeg nacionalnog značaja 2018. Beograd: Srpsko sociološko društvo, Institut društvenih nauka, Univerzitet u Beogradu, Filozofski fakultet, Institut za sociološka istraživanja.

10. Ljuboja, Dušan. 2015. "Balkanski migracioni procesi u 20. i 21. veku". Beograd: Center for International Relations and Sustainable Development (CIRSD).

11. Mitevska, Marija. 2022. "Sjeverna Makedonija na putu ekonomskog opstanka umjesto razvoja". Radio Slobodna Evropa. https://www.slobodnaevropa.org.

12. Mirilović, Filip. 2022. "Makedonski scenario". Vreme. Available from: https://www.vreme.com.

13. Popovski, Mihajlo, Naumova, Katerina. 2008. "TRAUMA AND POSTTRAUMATIC STRESS IN WAR IDPs IN MACEDONIA". Institute of Psychology, University "St. Cyril and Methodius" – Skopje, North Macedonia. https://scindeks-clanci.ceon.rs.

14. Radio Slobodna Evropa/CDM. 2022. "Mladi odlaze trajno: Migracije sa Zapadnog Balkana". Radio Slobodna Evropa/CDM. https://www.cdm.me.

15. Sotiroski, Kosta, Hristoski, Ilija. 2014. "Statistical Performances of Population Migration in the Republic of Macedonia at the Beginning of the 21st Century". U: *Migracijske i etničke teme.* 2014. https://hrcak.srce.hr.

16. Toshevska, Apostolovska, Biljana, Madjevikj, Mirjanka, Ljakoska, Marija, Gorin, Svemir, Radevski, Ivan, Dimitrovska, Olgica. 2018. "Republic of Macedonia – A Timeless Migration Mosaic". U: *Migracijske i etničke teme.* 34/2018.

17. Fazlagić, Admir. 2013. "Mladi Makedonci vide budućnost van zemlje". AlJazeera. https://balkans.aljazeera.net.

18. Wordlometers.info. 2022. "Republic of North Macedonia". Worldometers.info. https://www.worldometers.info.

Aleksandar Pavleski *)

UDC: 502.1
351.777

NEXUS BETWEEN ENVIRONMENTAL CHANGE AND SECURITY: DIMENSIONS, PRIORITIES AND CHALLENGES

Abstract: *In today's contemporary world, security is increasingly perceived as a variable category that means different things according to who talks about it, the enteties at risks and the nature of risks they identify as well. In this regard, the question arises about whether and in which way the environment can be set as reference security object and moreover, whether and how environmental change can be accepted as a generator of problems for national and human security. This paper analyses such effects and impacts of environmental change on security. Actually, through the prism of a broader theoretical and academic frame, the paper explores the interrelationships and dynamics between environment and security, with the main goal of recognizing and determining the impact of environmental change and environmental risks on security. Finally, regarding to such an analyze, the paper explores the main aspects and challenges for considering environmental change as a security issue.*

Key words: *environment, threats, risks, security, securitization.*

INTRODUCTION

A multitude of understandings and definitions about security are present in security theory and security studies. One of the reasons for such a situation arises from the fact that different researchers apply different starting points and approaches in security analysis and research. In this regard, an additional reason is related to the fact that security is a variable category and thus means different things with regards to who talks about it and the entities at risk and the nature of the risks they identify. Therefore, security should be perceived as a concept that needs to be specified by the context it is used in. However, in its broadest sense, security mainly implies freedom from threats.

*) Ass. Prof. Dr. Sc. Institute for Security, Defence and Peace, Faculty of Philosophy – Skopje, Ss. Cyril and Methodius University.

In the traditional aspect, the understanding of security is generally related to external relations among the states. Actually, the understanding of security in this regard is generally focused on the military threats. Military actions of a country against another harms the core values of independence and sovereignty. Moreover, military activities and endeavors also harm the lives of military personnel, as well as ordinary people. According to such notion of security (dominant during the Cold War period), security exists only in the absence of any direct military threats, which means that the environment is not included in such an understanding of security.

On other side, the so-called non-traditional understanding of security moves beyond physical and military threats and includes a wider range of tangible and intangible threats affecting human lives. Compared to the traditional security understanding, which considers security for the boundaries of the states and conflicts between countries, the non-traditional security understanding considers individual and community security. In this regard, non-traditional or critical security views have proposed several new security concepts, starting from the so-called human security to global security.

Human security refers to the protection from all threats that endanger human lives, which include hunger, poverty, disease and violence as well, while global security emerged as a response to the growing unprecedented threats of global warming, epidemics, international terrorism, etc. There isn't a country which can prevent and resolve itself alone such global issues and therefore the elimination of global threats and risks requires common action with participation of everyone, and not just a select few countries. Regarding to the research focus of this paper, it should be noted that environmental change as a security risk can be related to the both human and global security concept.

Actually, between these two concepts, additional concepts have been also developed in the past period, such as the following: environmental security, climate security, food security, pandemic security, energy security, cyber security, societal security, financial security etc. Such security concepts have directly

confirmed an evolutionary character of the security concept in the context of specific security environments. Actually, such security concepts are drawing the increasing attention in security research and on the security agenda, and the reasons in this regard are mainly related to the increasing frequency of non-traditional security threats and risks. In this regard, it should be noted that such concept of human security goes beyond physical security and now includes economic security, food security, health security and environmental security.
In the following section, the focus is specifically put on the analysis of the concept of environmental security, mainly through the prism of whether and how environmental issues are becoming security ones.

1. THEORETICAL ASPECTS OF THE ENVIRONMENTAL SECURITY

There are numerous interpretations of environmental security, depending on how the environment and security are understood themselves. Actually, during the last decades, the concrete ways of achieving environmental security within the global framework of sustainable development and security agenda have become an increasingly important subject of the international and academic debate. A multitude of high-level meetings, regional forums, international scientific conferences and other multilateral events have instigated public and academic discussion on the root causes of the global environmental crisis, its possible consequences for present and future generations, as well as possible approaches to rebalancing current (economic) growth, with responsibility for the whole planet.

However, regarding the research focus in the paper, it can be noted that the concept of the so-called environmental security is the product of the environmental movement and the changed strategic and security landscape by the end of the Cold War. The most important interpretations of the concept concern the ways in which environmental change puts national security at risk, the ways in which it may be a factor in violent conflicts, and the ways in which environmental change puts human security at risk.

The beginnings of theoretical debates and analyzes about the meaning and interconnection between the environment and security can be traced back in the 80's of the last century. Actually, researches linking environmental problems to non-traditional security concerns in this period tend to reject the state-centric and militarized definitions of security that dominated the security studies during the Cold War. They support the more holistic or "redefined" conceptions of security that extend beyond protecting the state from external aggression, arguing that global, regional, and local environmental problems seriously threaten human health and well-being and/or economic security (Lester 1977, 55). According to this line of thinking, it is in the common interest of all actors, not merely the states, to protect the world against environmental degradation for the same reason they must protect against organized violence: because both have the potential to harm human, material, and natural resources on a potentially large and disruptive scale (Stephen 1995, 175-207).

A significant step forward in the theoretical linking of environment with security has been made by the emergence and development of the Copenhagen School of Security Studies. Actually, contrary to the dominant, so called traditional/military security understanding during the XX century, the Copenhagen School of Security Studies approach is one of the most original attempts in promotion of a new (expanded and deepened) security understanding.

The expanded security understanding refers to the security understanding through the prism of five sectors: military, political, economic, societal and environmental, while in term of security deepening, in addition to the state, the importance of other reference objects have been emphasized, such as: the individual, society, the region and the world.

In this regard, the environmental security concerns the maintenance of the local and planetary biosphere as the essential support system on which all other human enterprises depend (Buzan 1991, 47). So, compared to previous theoretical

security approaches, the Copenhagen School has been understanding security through a broader and deeper approach, which includes military, political, economic, social and environmental security dimensions and aspects as well.

Regarding the aspiration for such a broader and deeper security interpretation and understanding, the representatives of the Copenhagen School have developed the so-called theory of securitization, which has a significant impact on the expansion of the security concept. According to such theoretical approach, security signifies a situation marked by the presence of a (security) problem and existence of a measure that can be introduced against it. Actually, threats are an integral part of everyday life and the daily functioning of states, but they become a security problem only in the absence of measures and activities to deal with them.

In the context of such theoretical approach, Wæver noted that each question/issue can be presented as following: 1) non-politicized – the state doesn't deal with the issue and it is not a part of the public debate; 2) politicized – the issue is part of a public policy and the government decides and provides certain means to address it; and 3) securitized – the issue is presented as an existential threat and it should be addressed as a priority issue which opened a necessity of extraordinary measures in dealing with it (Wæver et. al.1992, 90). It means that securitization process is determined by presence of an issue that is so urgent and existential, so that it is important to be dealt with decisively by the top leaders prior to other issues.

In this context, the term environmental security was launched to place the environment on the agenda of the so-called "high politics" (Grager 1996, 109-116). If one adopts a broad conception of security as "the means of people "that they will continue to enjoy those things that are most important to their survival and well-being" (Ronnfeldt 1997, 473-482), it can be plausibly argued that serious environmental degradation or change can indeed threaten security. This would be particularly true if the most serious warnings about global warming or holes in the ozone layer turn out to be correct, but even more traditional environmental

concerns like air and water pollution can threaten or kill more people than a smaller armed conflicts or even wars. In the political context, then it makes sense to give such issues a very high priority.

Taking into account the past and ongoing experiences and consequences of the environmental or natural threats and disasters (floods, droughts, earthquakes, typhoons etc.), it is no doubt that they can and should be perceived as an existential threat (especially for human life and health), with high priority for dealing with them. It practically means that, contrary to the previous approach about the abovementioned natural threats as the "acts of God", which resulted in a situation where they haven't been perceived as a subject of study or debate, the Copenhagen School and the Securitization theory have considered them as valid subjects of the study in the field of security studies.

Another important feature of the theoretical aspect of the interconnection among environment and security is the issue of access and control over natural resources. In this regard, Renner claim that, throughout the human history, and especially since the introduction of the system of sovereign nation states, struggles over access to and control over natural resources, … have been a root cause of tension and conflict and that history provides numerous examples of how states and nations were destabilized by environmental collapse leading to famine, migration and rebellion (Renner et al.1991, 109). Johan Galtung has also argued that "wars are often over resources" (Galtung 1982, 99), while Lothar Brock, asserts that "control over natural resources has always been important in enabling a country to wage war" (Brock 1991, 409). Sverre Lodgaard has also argued that "where there is environmental degradation, or acute scarcity of vital resources, war may follow" (Lodgaard 1992, 119). Regarding such understandings, it can be noted that access and control over natural resources may be perceived as a potent factor or factor of contribution to violence and thus threaten security in the sense of exacerbating open disputes or conflicts or by adding new dimensions to them.

2. SECURITIZATION OF THE ENVIRONMENTAL SECTOR

As mentioned above, the debate about environmental security (which dates back to the last two decades of the XX century) represents one of the first claims of broadening of security concept. Actually, according to the securitization theory, environment has become one of the five security sectors (besides military, political, economic and societal) of the broader security concept. In this regard, according to Buzan, the environment was recognized as one of the sectors that needed to be considered in their specificity for analyzing contemporary security dynamics (Buzan, 1991, 38).

The emergence of global environmental problems, such as global warming and ozone depletion, resulted in one of the first attempts to securitize the environment on a global scale. The Brandt Report (1980) suggested that 'few threats to peace and survival of the human community are greater than those posed by the prospects of cumulative and irreversible degradation of the biosphere on which human life depends' (Brauch 2003, 24). The World Commission on Environment and Development, in its 1987 report, recognized two major threats: (1) threat posed by the possible use of nuclear weapon; and (2) environmental degradation, as a present threat all over the world (WCED, 1987). In general, such new (environmental) threats implied the need to redefine the nature of security in an interdependent world facing new challenges.

One of the most striking features of the environmental sector is the existence of two different agendas - a scientific agenda and a political agenda (Buzan et al., 1998, 78). The scientific agenda, which is about the authoritative assessment of threat, refers to natural science and non-governmental activities. In fact, the scientific agenda consists of scientific and research institutions that investigate and analyze environmental problems. In that context, within this agenda, threats are assessed and a precondition is created for the securitization or de-securitization of an environmental issue.

On other side, the political agenda animates the public about environmental issues that are recognized by the scientific agenda and accepts political responsibility for solving such recognized issues. Actually, the political agenda creates public awareness of the problem and provides common instruments for solving it.

As most serious issues in the sphere of environmental security, around which the scientific and political agenda overlap, are perceived the following:

- disruption of the eco-system, climate change, deforestation, various forms of erosion, reduction of the ozone layer;
- energy problems, involving depletion of natural resources, nuclear disaster management, oil transportation problems;
- demographic problems, demographic expansion, epidemics, politically and socially uncontrolled migrations, urbanization;
- food problems, poverty, loss of fertile soil and water sources;
- economic problems;
- suffering of the civilian population as a result of military destruction of the natural environment, degradation of the environment by violence (Buzan et al. 1998, 74-75).

Within the securitization process in the natural environment sector, the reference object is the natural environment itself, as well as its connection with human civilization. From the securitization actor aspect, it is characteristic that in this sector, in contrast to the securitizing actors (those who emphasize the problem), there are also a large number of actors who prevent or limit the securitization process (mostly for the economic reasons). Functional actors, i.e. those who influence the dynamics in the sector, are mostly the economic entities, the chemical and nuclear industry, the fishing industry, etc. On the other hand, states and intergovernmental organizations that formulate certain rules for economic actors are also the functional actors within this sector.

Regarding the securitization concept, there are three major groups of threats to the natural environment: 1) threats to human civilization that arise from the natural environment and that are not caused by human activity (earthquakes, volcanoes, meteors, etc.); 2) threats from human activity to the nature or structure of the Earth, when the changes that are caused create an existential threat to the humanity (greenhouse gas emissions, ozone depletion etc.); and 3) threats from human activity to the nature or structure of the Earth, when the changes caused do not create an existential threat to humanity (Georgieva 2006, 57).

In general, security dynamics in the environmental sector are complex for several reasons. First of all, the dilemma is always open about the way a specific environmental problem will manifest itself and whether it will be politicized or securitized. The opponents of securitization in this sector, as well as the motives of the functional actors, represent an additional challenge. Even more, the situation may become more complicated if the environmental problems are linked to certain structural problems in society.

3. NEXUS BETWEEN ENVIRONMENTAL CHANGE AND SECURITY: DIMENSIONS, PRIORITIES AND CHALLENGES

After a long period of debate and analysis about environment and security, nowadays, there is a much clearer understanding regarding how environmental changes affect security concerns. In this sense, it should be noted that long-term environmental degradation is not a major or pervasive cause of international wars, ethnic wars, or revolutionary conflicts. Such degradation often brings misery and can exacerbate local tensions and conflicts in a society, yet such misery does not generally trigger the elite alienation and opposition necessary for large-scale violence to occur. Short-term disasters, however – floods, hurricanes, droughts, earthquakes and major accidents – can contribute to major political conflicts if

elites and popular groups blame the regime for causing or for a particularly poor or corrupt response to such disasters. In addition, where environmental resources represent concentrated and scarce sources of wealth, then even if those resources are not degraded, conflict over control and exploitation of those resources can be a source of internal violence.

Actually, environmental change poses risks to the territorial integrity and economic growth of the states, as well as to the health and welfare of people and communities, and it may increase the risk of violent conflict. Therefore, environmental change can be perceived as serious risk for national and human security. Regarding the trajectory of the so-called environmental insecurity, it should be noted that the broad history of human-environment relations and interactions has been the one of the increasing population growth, increasing use of resources per capita and increasing inequality between the richest and poorest people in the world in terms of consumption and pollution. These trends, combined with the development of industrialization as the dominant mode of production, capitalism as the near-universal economic order, and the centralized control of the means of violence (mainly by the state), have given rise to a condition where environmental change increasingly poses risks to people, states, and peace (Giddens 1985, 79).

The world's population has rapidly grown from 2.5 billion people in 1950, to around 6.7 billion in 2008 and will most likely peak at 9 billion people in 2050 (Boyden 1987, 2-3). The vast majority (80 %) of people live in developing countries. Such a growing world population has directly affected bigger production and consumption of needed products for normal human existence. This, this directly produced greater use of resources, which in turn has initiated significant environmental pollution. In many states, population and environmental changes together combine to produce environmental changes with global impact. That is in countries with large populations and large or rapidly increasing levels of per capita

such an environmental impact (such as carbon dioxide output, forest reduction, natural habitat destruction and colonization), and thus environmental changes occur with global implications for security (Goldstone 2001, 46).

In addition, although overall population growth and population density do not directly predict political risks, still, a number of distinct types of demographic changes – particularly the rapid growth in the labor force, shifts in the age distribution, unequal population growth rates between different ethnic groups, urbanization that exceeds employment growth and migrations that change the local balance among major ethnic groups – do increase the risks of violent internal political and ethnic conflicts.

Poverty is also a powerful driver of vulnerability to environmental change, as the poor have few means at their disposal to avoid, reduce or adjust to risks to livelihoods created by environmental changes. In an average day, environmental degradation and poverty combine to cause the death of 5,200 children due to diarrhea, and 2,300 children due to malaria (Bryce 2005, 33). Undernutrition is an underlying cause of over 4.6 million child deaths each year (Black et al. 2008, 140), and inadequate access to clean water and sanitation results in the deaths of 1.4 million children each year (Bartram 2005, 89). As a result of the abovementioned, it is no doubt that the combination of poverty and environmental change is producing environmental insecurity, which is the vulnerability of individuals and groups to critical adverse effects caused, directly or indirectly, by environmental change. In this regard, environmental security is achieved only in cases when individuals and groups have the ability to avoid or adapt to environmental change so that their basic needs, rights, and values are not undermined (Barnet 2001, 120).

Climate change is another significant aspect of vulnerability to environmental change that is especially a characteristic of the so-called developing countries.

Actually, the previous experience shows that climate change has potential to disrupt development in such countries. It is a result of their limited capacities for prevention and dealing with the impact of extreme weather conditions from one side, and their mostly economically dependency on climate sensitive sectors like agriculture, forestry and tourism, on the other (Wade and Jennings 2015, 89-90). However, it should be noted that the very imminent impacts of climate change are not felt only trough rising temperatures. Rather, these effects come in the form of changes in the hydrological cycle. For example, changes in the average volume of annual precipitation can lead to increases in the number of torrential rainfalls, thus causing flood. Likewise, the decrease in the number of rainy days increases droughts (Ludwig et al. 2007, 48-56).

Climate change-related events have already grown into a major driver of migration, forcing families and communities to flee, mostly as a result of water scarcity, crop failure and sea level rise (Barron 2018, 67). In general, these events are expected to increasingly continue do displace people, especially in the developing countries. It is specific that such a displacement is usually interconnected with several risk factors, such as the following: homelessness, landlessness, loss of access to common property, food insecurity, joblessness, marginalization, social disintegration, etc. In fact, such factors are recognized by the conflict theory as part of the structural causes that can lead to the emergence of violence or that can seriously affect the dynamics in an existing conflict environment. It follows that the climate change consequences can also be perceived as serious security risks and threats. In this regard, the International Organization for Migration (IOM) has estimated that future effects of climate change could create 25 million to 1 billion of environmental migrants by 2050, moving either within their countries or across borders, on a permanent or temporary basis, and 1-2 billion by 2100, which could accelerate the existing conflicts or even create new ones (IOM, 2022)

Environmental scarcity also presents a significant aspect of the nexus between environmental change and security. Actually, environmental scarcity and its interactions produce several common social effects, such as the following: lower agricultural production (which can affect food security), migrations from the zones of environmental scarcity (which can affect societal security or identity security), weakened institutions (which can be related to the risks of political security). However, the influence of these social affects in threating above mentioned security types is mainly determined by people or group perception about the existing of relative decrease in their living standards compared with other groups, or compared with their aspirations (Gurr 1993, 54).

Still, high levels of people grievance about the environmental scarcities do not necessarily lead to the widespread civil violence. Actually, civil violence, that is in general a reflection of troubled relations between the state and the society, is triggered by at least two other factors: groups with strong collective identities that can coherently challenge state authority, and clearly advantageous opportunities for violent collective action against authority. So, the aggrieved must see themselves as members of groups that can act together and they must believe that the best opportunities to successfully address their grievances involve violence.

However, there is no doubt that the presented environmental scarcities can threaten the complex relationship between the state and the society, as well as between two or more states. Falling agricultural production, migrations to urban areas (or to other states), and the reduce of economic productivity often produce hardship, and this hardship increases demands on the state. In such situations, it is no doubt that environmental scarcities can lead to the emergence of serious resentment that can even initiate violence.

CONCLUSION

In this paper, the author presented an analysis about the nexus between environmental change and security, involving multiple aspects of the ways in which environmental issues become security ones. In this regard, the presented analysis confirms that the relationship between environment and security, which has garnered increased importance since the end of the Cold war, has a complex nature, thus initiating the necessity of applying comprehensive approach in understanding such an interconnection. As mentioned above, environmental change and degradation haves various impact on the behavior of the involved actors and might play a role as reason, trigger, channel and catalyst of worsening security dynamics. It is no doubt that the decrease in quantity and quality of resources, rapid population growth, climate change and the unequal resource access are the basic drivers behind the increasing environment-related security risks. In addition, scarcity of nonrenewable resources can also contribute to changing the security dynamics in the national, as well as in the international context.

On the other side, the analyzed securitization process within environmental sector also shows the existence of complex dynamics, especially in term of the way in which a specific environmental problem will be presented and whether it will be politicized or securitized. Moreover, the opponents of securitization in the environmental sector, as well as the functional actors' motive and possible connection of environmental problems with certain structural problems in society, represent an additional aspect of such complexity.

In general, it can be concluded that there are multiple aspects that create the complex dynamics of the relationship between the environment and security. Among others, the most important are the following: 1) the fact that environmental change, pollution and disasters transcend national boundaries, which means no state is immune to this process; 2) the fact that the threats are the result of both

human activity and the flows of the nature itself; 3) the fact that there are numerous actors involved in the securitization process of environmental sector; 4) the fact that economic development is inevitably determined by the functioning of industry, which in turns produces negative environmental change and effects; 5) dynamic lifestyle increasingly imposes a need for fast transport of people, goods and services today, which has also negative environmental effects.

It can be also concluded that, in general, environmental and demographic change can produce security problems of two distinctly different kinds. The first one, the so-called violent environmental security issues, reflect the impact of demographic and environmental changes on traditional security concerns, that is, the ways that demographic or environmental changes increase the risk of violent international or domestic conflicts. On other side, the so-called nonviolent environmental/demographic security issues reflect the changes in population or in the environment (emissions that damage the ozone or contribute to global warming, activity that reduces biodiversity, etc.) that have consequences across international borders that produce undesirable outcomes and thus become the issues of international security, even if they are not likely to produce violence.

As a result, it can be concluded that, because of its nature, environmental security is a complex category that reiterates the necessity of applying comprehensive approach both by state and non-state actors, when speaking of dealing with and preventing environmental risks and threats.

REFERENCES

1. Barnet, Jon. 2001. *The Meaning of Environment Security: Ecological Politics and Policy in the New Security Era.* London and New York: Zed Books.
2. Barnet, Jon. 2010. Energy Security. *The Routledge Handbook of New Security Studies*. New York: Routledge.
3. Barry, Buzan. 1991. *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*. Hemel Hempstead. Harvester.
4. Barry, Buzan, Ole, Wæver and Jaap, De Wilde. 1998. *Security: A New Framework for Analysis*. Lynne Rienner Publ. Colorado.
5. Brauch, Hans. 2005. *Environment and Human Security: Towards Freedom from Hazard Impacts*. Bonn: Institute for Environment and Human Security.
6. Brock, Lothar. 1991. Peace Trough Parks: The Environment on the Peace Research Agenda. *Journal of Peace Research* 28(4): 407-423. SAGE Publications.
7. Brown, Lester. 1977. *Redefining Security*. Worldwatch Paper No. 14 Washington, DC: Worldwatch Institute; Ullman.
8. Deudney, Daniel. 1991. Environment and security: muddled thinking. Bulletin of Atomic Scientists. April 1991.
9. Finger, Matthias. 1991. The military, the nation state and the environment. *The Ecologist* 21: 220-225.
10. Galtung, Johan.1982. *Environment, Development and Military Activity. Towards Alternative Security Doctrines*. Oslo: Norwegian University Press.
11. Georgieva, Lidija. 2006. *Risk Management*. Faculty of Philosophy. Skopje.
12. Giddens, Anthony. 1985. *The Nation-State and Violence*. Los Angeles: CA – University of California Press.
13. Goldstone, J. (2001). Demography, Environment and Security. *Environmental conflict*. Westview Press.

14. Grager, Nina. 1996. Environmental security? *Journal of Peace Research*, Vol. 33, No. 1, pp.109-116. SAGE Publications.

    a. Lodgaard, Svere. 1992. Environmental Security, World Order and Environmental Conflict Resolution. *Conversion and the Environment*, pp.115-136, ed. Nils Petter Gleditsch. Westview Press.

15. Paul, Diehl, and Nils Petter Gleditsch. 2001. *Environmental Conflict*. Westview Press.

16. Renner, Michael, Mario, Pianta, and Cinzia Franchi. 1991. International Conflict and Environmental Degradation. *New Direction in Conflict Theory*. pp.108-128, ed. Raimo Vayrynen. London.

17. Ronnfeldt, Carsten. 1997. Three Generations of Environment and Security Research. *Journal of Peace Research*, Vol.34, No. 4, pp.473-482. SAGE Publications.

18. Wæver, Ole, 1995. Securitization and Desecuritization. In: Lipschutz R.D. (ed) *On Security*. Columbia University Press, New York.

Dušan Proroković*)

UDC: 620.9:355.45
620.91(470+571):327(4-672ЕУ)

RUSSIAN ENERGY SOURCES AND THE EU SECURITY POLICY

Abstract: *It is impossible to plan EU security policy without ensuring energy security. Stable access to energy sources is the basis for creating economic policy. Considering the importance of the EU for the whole of Europe, it is impossible to ensure continental security without the EU energy security. The thesis that it is necessary to reduce imports and rely on one's own resources has been present in the EU projections for years. However, little has been done in this regard. Europe's security still depends on Russian energy, regardless of announcements of the EU officials that a different scenario is possible by 2027 or 2030.*

Keywords*: EU, Russia, NATO, USA, energy security.*

INTRODUCTION

Energy relations between Russia and European countries have a long tradition. At the end of the 1960s, the export of Soviet oil began, and in 1967 the Dolyna-Uzhhorod-Western border of the USSR gas pipeline was completed, which created the prerequisites for distribution to consumers in Central and then Western Europe. We should take into account the fact that part of today's EU members were either in the Soviet Union (Estonia, Latvia, Lithuania) or in the Eastern Bloc (Czech Republic, Slovakia, Poland, Hungary, Romania, Bulgaria, including East Germany) and therefore, they were practically integrated into a single huge system, within which they could first buy oil at lower prices (it was the way the USSR helped its allies), and then also implement the project of mass gasification of the economy and households. Hence the great dependence of all the mentioned countries on Russian energy sources. The connection with the oil wells in the east was planned with oil and gas pipelines that passed through the territories of Ukraine and Belarus. The collapse of the USSR accelerated the strengthening of energy ties between Russian producers and Western European consumers. On the one hand, in the long period of transition (during the 1990s) and then in the phase of *re-sovereignation* during the first two presidential terms of Vladimir Putin (2000-2008), the Russian economy relied on the energy sector, first for "filling the

*) Research Fellow at the Institute of International Politics and Economics, Head of the Center for Eurasian Studies, Belgrade, Serbia. E-mail: dusan@diplomacy.bg.ac.rs.

budget", and then for the formation of an investment mass that will be used to start infrastructure projects and the economy. Excluding a few other economic branches, which were again connected with the exploitation of natural resources (such as, for example, coal mining in the Kuznetsk basin in the southeastern Siberia on an area of about 26,000 km^2; production of nickel and copper, which predominantly refers to the city of Norilsk on Taimyr in the Arctic Circle; steel production in Magnitogorsk in the Chelyabinsk region, etc.), there were no other solutions for post-Soviet Russia. On the other hand, for Western European countries, Germany and Austria in the first place, as well as Italy to a large extent, and to some extent France, it was important to have a stable distributor in their immediate neighborhood, who would deliver cheap crude oil and natural gas, in the agreed quantities and respecting the delivery dates. In the post-Cold War world, European countries, and Germany in the first place, as the "economic engine" of the Old Continent, saw two benefits from this cooperation. First, as far as the import of crude oil is concerned, they became less dependent on American acquisitions and their distributors (either those from the Middle East, or those from the USA and Canada). In perspective, this meant greater independence in projecting economic dynamics, and thus also in the process of making political decisions. Second, the binding of European industry to cheap and ecologically clean natural gas as a key energy source increased the competitiveness of the European economy on a global scale.

Map no. 1: Gas pipelines connecting Russia and the EU via Ukraine and Belarus

1. ENERGY SECURITY OF EUROPE AND RUSSIA

Mutual interest eventually led to the need of building a new main pipeline, which manifested in the development of ideas about the North Stream, and then the South Stream (Smith 2011). In addition, natural gas is distributed through the Progress and Soyuz pipelines, which include as many as 22 regional gas pipelines with 72 compressor stations, horizontally east-west (border with Russia-border with Slovakia and Hungary) and through the Yamal gas pipeline (Yamal is stretching through the territory of Belarus, from Russia to Poland, but is connected with the northwestern branch of the Ukrainian gas pipelines), while crude oil is transported by the Druzhba pipeline (Pirani 2007, 17-18).

Thus, Russia became the EU's main supplier of crude oil and natural gas, as well as of solid fossil fuels used for the production of electricity in thermal power plants (located in the Kuzbass). Not even the continuous deterioration of political relations, which occurred after the escalation of the Ukrainian crisis in 2014, could have disrupted this. "In 2020, almost three-quarters of crude oil imports outside the EU came from Russia (29%), the USA (9%), Norway (8%), Saudi Arabia (7%) and Great Britain (7%), as well as Kazakhstan (6%) and Nigeria (6%). A similar analysis shows that more than three-quarters of natural gas imports into the EU came from Russia (43%), Norway (21%), Algeria (8%) and Qatar (5%), while most of the coal imports came from Russia (54%), followed by the USA (16%) and Australia (14%)" (Eurostat April 2020). Otherwise, in the structure of energy imports into the EU, about two thirds are oil and oil derivatives, 27% natural gas and 5% solid fossil fuels.

Despite the widespread promotion of the *Green Agenda* and political aspirations to "free Europe from fossil fuels", not much has changed in the first two decades of the 21st century. "The dependence rate shows the extent to which the economy relies on imports to meet its energy needs. It is measured by the share of net imports (imports-exports) in gross internal energy consumption (which means the sum of produced energy and net imports). In the EU in 2020, the dependency rate was equal to 58%, which means that more than half of the EU's energy needs were met by net imports. This rate is lower compared to 2019 (60%),

which is partly related to the economic crisis of *Covid-19*, but is still slightly higher compared to 2000 (56%). In the member states, the rate of dependence on imports ranges from over 90% in Malta, Cyprus and Luxembourg to 10% in Estonia. In 2020, the EU was mainly dependent on Russia for the import of crude oil, natural gas and solid fossil fuels, followed by Norway for crude oil and natural gas" (Eurostat April 2020).

Looking at the crude oil market alone, "European dependence increased from 76% in 2000 to over 88% in 2014. The EU spends around 215 billion euros on oil imports, over 5 times more than on gas imports (40 billion euros). Russia is the largest supplier: dependence on Russia increased from 22% in 2001 to 30% in 2015" (Buffet 2016). Among the ten largest individual companies that export oil and oil derivatives to the EU, there are as many as three Russian companies, among them the first two places are occupied by Rosneft (20%) and Lukoil (12.5%), while Gazpromneft is in the ninth place (close to 5%). When it comes to importing natural gas, Finland imports from Russia as much as 94% of its total needs, Bulgaria 77%, Slovakia 70%, but what is a particularly sensitive issue is that the three largest "continental economies" import significant contingents - Germany 49%, Italy 46% and France 24% (it should also be added that Poland, as the fifth most populous member of the EU and a country important for regional security, imports about 40%). (Buchholz 2022).

The topic of Europe's energy security is inextricably linked to the issue of energy distribution from Russia. Since February 2022 and the beginning of the war in Ukraine (in Western countries this event is labeled as "aggression" or "invasion" of Russia on Ukraine, and in Russia as a "special military operation"), attempts to reduce the dependence of European consumers on Russian producers have been noticeable. In this context, the EU adopted as many as seven packages of sanctions against Russia, of which the fifth package is specifically oriented towards the energy sector (it refers to the complete stop of purchase of solid fossil fuels from Russia, as well as crude oil, excluding the contingent distributed by oil pipelines). With that, they want to ensure the energy and overall security of the EU (as well as the whole of Europe) without relying on Russia. To what extent is it possible to project the security of Europe without Russian energy sources?

2. EU SECURITY POLICY

All seven packages of sanctions (agreed on until August 2022, when this article was written; it does not rule out that there will be more in the following period) against Russia were formulated within the Common Foreign and Security Policy of the EU. "The European Commission uses the Common Foreign and Security Policy budget to respond in a rapid and flexible manner to external conflicts and crises, to build the capacity of partner countries and to protect the EU and its citizens" (European Commission 2022).

Looking from the point of view of the declared principles, the EU therefore wanted to use sanctions to force Russia to take a different position in the Ukrainian crisis (stopping armed actions, disrupting the economic situation in Russia, which would put pressure on the leadership in Moscow, causing social and political protests in Russia, etc.), thus achieving a certain political advantage and improving its political and negotiating position. How realistic such assessments were and what their consequences are is a completely different matter. For this research, it is important to ask the question: where did the idea come from within the EU to undertake something like this in the energy sector? Because, as stated in the introductory part, not only in previous years, but in previous decades, absolutely nothing indicated that such a sudden turn could occur. The energy security of the member states (therefore also the economic security), and it should be repeated that we are firstly thinking of Germany, and to a certain extent Italy and France, is designed on cooperation with Russia and the accessibility of cheap natural gas. It became the basis for increasing the competitiveness of the EU economy in the global economy, ensured continuous economic growth, low unemployment, high wages and political stability. Almost nothing was done to change that, on the contrary – the connection with Russia was strengthened and deepened, a classic example being the construction of two lines of the Nord Stream gas pipeline (See more in: Turksen 2020).

In truth, the EU has declared greater energy independence as a political goal through a series of documents. The focus is on the *Green Agenda* and renewable energy. However, little has been done in this regard (the question is how much could be learned in a short period of time), and dependence on imports remained high. The insistence on constantly repeating the thesis of energy independence in the European Common Foreign and Security Policy came from the other side. It is impossible to see the security policy of the EU without NATO. And when it comes to NATO, there is a completely different view on Russian energy sources within this organization. The fact that Russian energy resources in Europe are a problem for NATO becomes obvious in the *NATO 2020 Strategic Concept*, whose design began in 2009 (it was adopted a year later) (NATO 2010).

The new solutions defined in the *NATO 2020 Strategic Concept* (the expert team for writing the document was led by Madeleine Albright) partly state the fact that the previous Washington Strategy did not bring the expected result, since instead of promoting human rights and democratic values, the dominant themes became firstly energy security, and then the reliability and protection of information systems, environmental problems and curbing demographic growth. Changes in the field of finance and economic activity represented special problems as well. The West is still the most economically important part of the world, but nowhere near the dominant position it had mid-1990s.

The *NATO 2020 Strategic Concept* also raised the issue of NATO-EU relations. Within the EU, instead of the previous category of Common Security and Defense Policy, the Lisbon Treaty of 2007 clearly foresees the "possibility of creating a common European defense" (European Commission 2007), and what exactly this may mean in the future remains open. The authors of the proposal for the new NATO strategic concept therefore warned that no room for double interpretations should be left and that "the Lisbon Agreement must serve the purpose of further strengthening NATO" (NATO 2010). In order to ensure tighter integration and prevent the creation of new problems, a number of internal structural changes are proposed. Acceptance of the mentioned measures would mean that NATO member states would give up another portion of their own

competences in favor of common (super)organs of the alliance and strengthening the influence of the US, which has undisputed dominance in common bodies. (NATO 2010)

That is why, on the one hand, the *NATO 2020 strategy* directly binds Article 4 and Article 5 of the North Atlantic Treaty. Article 4 talks about cooperation and coordination, and Article 5 about the principle of "all for one-one for all", whereby all members of the Alliance are obliged to defend an attacked ally (NATO 1949, Art. 4, 5). By placing these two articles in direct dependence, the USA warned the other members that if they want protection, they must cooperate more. Cooperation implies that they would not look favorably if there would be a repetition of the situations from 2003 during the attack on Iraq or the Russian-Georgian war in 2008 when NATO couldn't take a unified position. Hence, in spite of the moderate opposition of some members and the fierce criticism of the opposition in Germany and France, the unquestionable following of the USA regarding its stance towards Russia since the escalation of the Ukrainian crisis remained until today. The European members of NATO have agreed to this kind of relationship, they have committed themselves to simply go beyond certain goals established by the Lisbon Treaty and act against Russia even when it causes direct damage to the EU (for example, the introduction of sanctions that caused a dramatic drop in exports of agricultural products from the EU to Russia) in order to protect their own security and their relations with the USA (See more in: Smith 2010)

The reasons for such an aggressive performance should not be sought only in the consolidation of Russia's position since 2008, but also in the long-term projected initiatives on the energy connection of Russia and the EU. The *NATO 2020 Strategic Concept* opens the issue of energy security of European members and sets it as one of the priorities.

At that moment (the observed period is 2006-2009), 180 billion cubic meters of gas were delivered from Russia to other European countries through the already existing gas pipelines, plus another 9 billion cubic meters that Russia delivered to Finland through the joint Russian-Finnish gas pipeline. It is planned that another 16 billion cubic meters should be delivered from Russia to Turkey via the Blue

Stream gas pipeline, with a planned growth of up to 32 billion by 2030, as well as around 30 billion cubic meters per year through Germany to Western Europe via the North Stream gas pipeline, with growth up to 55 billion until 2030; moreover, up to 30 billion cubic meters of gas are delivered annually to Southern and Central Europe via the two branches of the South Stream, which would bifurcate in Bulgaria (Bariš 2009, 13-14, 93-95).

Placing the issue of energy security of European members high on the list of priorities is motivated by attempts to prevent the strategic linking of Russia and the EU.

3. ATTEMPT OF "ENERGY SEPARATION" OF THE EU FROM RUSSIA – ALTERNATIVES AND PERSPECTIVES

The proposals of the USA to make NATO the guarantor of European security in a new way and the obligation of European members to participate in it are linked to the assessment that, with less dependence on the American energy distributors, the key countries of continental Europe (Germany, France, Italy) were becoming more independent in the process of adopting political decisions. NATO still existed as a defense alliance, but the EU increasingly acted economically and politically as it suited it. The diplomatic conflict with the US over the intervention in Iraq in 2003 caused concerns in Washington, because it was the first signal that Western Europe would not follow the US always and everywhere in the way it did before (FR Yugoslavia, Afghanistan).

One of the ways of the new subjugation of Europe was to make it dependent on energy imports from American distributors or their allies, as it was done during the Cold War period. While, on the one hand, the "Russian energy products" were declared the enemy's "geopolitical weapon", on the other hand, alternative ways of supplying the European market with crude oil and natural gas were devised. It is, in fact, a response to the *Russian Energy Strategy until 2020*, which was adopted in 2003 (Bushuev & Troitskii 2007, 1-7). Even then, the USA recognized what they half a decade later called the "malignant Russian influence", which being

spread through Europe through strategic pipelines. Next to the USA, Russia is by far the largest producer of gas, the country with the largest confirmed gas reserves, the largest producer of crude oil along with Saudi Arabia, and with all that, the largest military nuclear power in the world. It was a challenge to US national security, and it was classified as such in a large number of official documents adopted since 2005.

President Donald Trump declared the following in June 2017: "Our goal is energy dominance". It goes without saying, on a global scale. But what was completely openly and unequivocally announced by President Trump, was actually prepared for a long time within American institutions (Proroković 2019, 114-134).

The change in the American approach was visible immediately after the election of George W. Bush as president in 2000. In parallel with the initiation of the Second Gulf War and the intervention against Iraq, the US tried to influence the global energy market by controlling the "sources" and initiating the construction of strategic pipelines. It primarily concerned connecting European consumers and Middle Eastern producers. The transition from oil as the most sought-after energy source to the natural gas as "cleaner" and more available in the future, was already underway.

Map. no. 2: Planned route of the Nabucco gas pipeline[29)]

[29)] Taken from the following internet page: http://www.nabucco-pipeline.com.

Estimates are that oil consumption at the global level will increase, while reserves will decrease (Đukić 2009). West European countries, which import about 70% of this energy source, are particularly interested in gas as end-users. Depending on which energy source is observed – crude oil or natural gas, the approach to defining energy security goals also differs. The largest crude oil reserves are located in the Middle East (Venezuela and Saudi Arabia have the largest confirmed reserves individually), but there are also significant sources in the wider Caspian Lake region and in Russia, while the largest natural gas reserves are located in Russia (confirmed reserves of 47 trillion cubic meters) and Iran (28.5 trillion cubic meters). For this reason, the US is increasingly beginning to view Russia and Iran as "challengers" in the world politics.

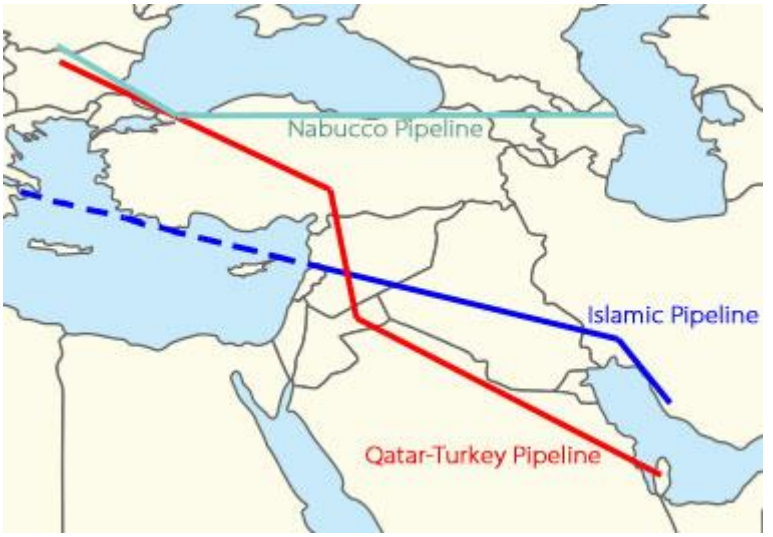
Hence the launch of the 'Nabucco megaproject' (NABUCCO pipeline). This strategic pipeline would, as planned, "start in Azerbaijan and deliver gas to the rest of Europe via Georgia, Turkey, Bulgaria and Romania. The length of the gas pipeline should be 3,893 kilometers, and the capacity should be 31 billion cubic meters. Although it was noisily announced, the realization of 'Nabucco' did not begin at all. In July 2013, it was announced that the main planned supplier - Azerbaijan, was withdrawing, and before that, German investors also withdrew from the project. So, instead of 'Nabucco', a talk started about the 'Trans-Adriatic Pipeline', which would transport gas from the Shah-Deniz field in Azerbaijan to southern Europe. The 'Trans-Adriatic gas pipeline' would stretch 870 kilometers from the Greek-Turkish border in the northeast, through northern Greece and southern Albania, then along the bottom of the Adriatic Sea to southern Italy. It would be connected to the 'Trans-Anatolian Pipeline' on the Greek-Turkish border, which should be completed by 2018, and initially it will bring about 16 billion cubic meters of gas per year to the 'Trans-Adriatic Gas Pipeline'. However, in the case of the 'Trans Adriatic Pipeline' the same question arises as in the case of 'Nabucco', because there is a constant concern whether the gas from Azerbaijan

is an adequate alternative to the main reserves from Russia (which is part of the EU's efforts towards a larger energy transition) that is - whether the volumes from Azerbaijan are sufficient on their own" (Proroković & Perović 2013, 124-125).

Without relying on sources in Iran or Qatar, the 'Nabucco' gas pipeline could not have been realized, and therefore the *Bush Doctrine* was paralyzed. However, there were two other plans considered for Iran and Qatar: 1) Gas pipeline Turkey - Qatar; 2) Islamic gas pipeline. (Map no. 3). Due to political instability and security challenges, neither of these two plans was further developed.

The originally considered route through Saudi Arabia, Kuwait and Iraq was difficult to imagine because of the problems in Iraq, i.e., the position of the (Iraqi) Kurdistan, while the second one, through Saudi Arabia, Jordan and Syria, remained only in the plans because the Syrian authorities resolutely refused to participate in that project (with the support of Russia and Iran) (Carlisle 2009). One of the reasons for the start of the civil war in Syria should be found in this.

Although the USA insisted at the NATO Summit in Bucharest in 2008 that in the final document the issue of energy security of European countries should be one of the priorities, and "displacing Russian energy influence" one of the most important tasks, by paralyzing the *Bush doctrine*, little could have been done at that moment (NATO 2008). Contrary to the insistence of the USA, Russia has already extensively planned the construction of two natural gas corridors – North Stream and South Stream, so Europe's dependence on Russian gas would become even greater. In any case, partly because of the failure of the *Bush doctrine*, and certainly because of the American intervention in the Middle East, the price of oil and gas started to skyrocket. By 2003, the price of a barrel of crude oil hovered around $30, then by 2005 it had risen to $50, before exploding to an all-time high in August 2008 of $147.30. From 2008-2014, the price of oil ranged from 70-120 USD. For the US, it was, and it is problematic for two reasons.



Map. no. 3: Planned routes of the Qatar – Turkey Pipeline and Islamic Pipeline

First, in numerous analyses, the increase in energy prices is directly linked to the global recession (Kliesen 2001). Since the USA accounts for about 22-23% of the world GDP, such disruptions are a primary threat for them. That's why the USA had to increase production, become less dependent or completely independent from the OPEC countries and Russia. The USA wants to be dominant in creating prices on the world market, and it will be able to do so not only by increasing or reducing demand, but also by increasing the supply. Secondly, among the oil and gas producers, there are also countries with which the US does not have good relations or which it anticipates as global or regional challengers to its interests. This primarily refers to Russia, Iran, Venezuela, Algeria, Syria, Sudan, but also China, which is the largest importer, but at the same time the sixth largest producer of oil in the world, and Brazil, which is in tenth place. The higher price of oil and gas stabilized the political and economic conditions in these countries, but also enabled them, due to the budget surpluses that occurred, to increase their military power, investing in the military-industrial complex or buying new weapons and equipment.

All the attempts of the US to achieve "energy dominance" failed until 2014, even produced counter-effects as the rise in energy prices on the global market caused the Great Economic Crisis (began in 2008-2009, but its consequences began to become more visible in the second decade of the 21st century), which harmed the "collective West" the most, and contributed to the consolidation of budget revenues of challengers in the international arena, among which Russia profited the most. Since the desired reorientation of European consumers from Russia to producers in the Middle East (Iraq, Qatar, Azerbaijan, Saudi Arabia) did not occur, it was not possible to organize an alternative sustainable supply chain. NATO's strategic conception defined one thing, but in practice, something else took place.

The new project of "separating Europe from Russia" was therefore initiated during the second term of Barack Obama, and later continued by Donald Trump, this time by devising the concept of liquid petroleum gas supply. In order to reduce dependence on Russian gas, a new strategic project was presented at the summit in Warsaw back in 2016 – connecting the terminal for liquefied petroleum gas on Krk, which has yet to be built, with the existing terminal in Swinoujscie, Poland. Vertically north-south, from the Baltic Sea to the Adriatic Sea, Central-Eastern Europe would be networked in a new way (Proroković 2018, 57-58). This project is still being insisted on, and it experienced a kind of renaissance after February 2022. Since then, the policy of reducing energy dependence on Russia has been concretized, manifested in a completely different way than before. The EU accepted everything that was considered and adopted within NATO, and thus liquefied petroleum gas was declared a valid alternative.

Ursula von der Leyen, the president of the European Commission, is in favor of ending the purchase of Russian energy products in the next five years, and announced a plan (which will be harmonized with the measures that will be adopted in the meantime, including the sixth package of sanctions) according to

which crude oil and natural gas from Russia were to be phased out by 2027. The proposal of the European Commission is less optimistic and foresees the fulfillment of this goal by 2030.

However, three open questions arise regarding this. The first and most logical is – where will the EU buy energy sources (due to the relatively smaller share of coal in the EU's energy balance, as well as for the fact that the members still have reserves that they have not used, this resource can still be replaced)? This question is raised both in the short and medium term (it is necessary to ensure the import of crude oil and natural gas until 2027 or 2030, but an issue should be raised as well regarding how can this matter be solved after that time-frame). Energy sources are bought with long-term contracts, and growing Asian economies (China and India in the first place) have already reserved significant quantities for the next period with the producers in the Middle East and Africa. Similar thoughts have been existent in the EU for the last two decades, and were especially intensified after 2014 and the deterioration of political relations with Russia, but the figures shown show that an alternative to imports from Russia has simply not been found. In political speeches and journalistic analyses, the import (and production) of liquefied petroleum gas (from the USA and Qatar) is mentioned as an alternative solution, but these announcements are not accompanied by elaborations on the feasibility of the necessary quantities and possible prices (therefore the profitability of the project).

One cannot talk about implementation of the *Green Agenda* with a drastic increase in the production of liquefied petroleum gas in the USA (and potentially - European countries), bearing in mind the methods of production that devastate the environment (fracking technology).

Another issue is the price of the energy that will be procured in this way. The new calculation implies abandoning the distribution of resources by pipelines and

the use of tankers and new installations that will be built (large investments are necessary, and such a method of distribution always costs more). At the same time, if the purchase of Russian energy products is abandoned by a political decision, the participation of the largest suppliers in the market until now is also prevented, thus raising the price to a completely new level (for example, China will now "compete" for oil from the Middle East in the market competition with India, the USA, EU and other smaller countries, which will make the resource more expensive, because higher demand means higher prices). Again, unlike China and India, as well as a whole series of other actors from the non-Western part of the world who will buy Russian energy products and thus will not give up the market mechanism for lowering the price, the EU will no longer have that exclusivity, which can have a very negative impact on the competitiveness of the European economy.

The third question is related to Russia's reactions and countermeasures. Just as the US and the EU are waging a hybrid war against Russia, Russia is also waging a hybrid war against the US and the EU. One of the unconventional means used in this conflict are the energy sources. On the one hand, with the outbreak of the armed conflict in Ukraine, and the deterioration of relations between the West and Russia, the prices of energy products began to rise (natural gas rose in price many times, reaching historical highs). In addition, political messages from Moscow are constantly being manipulated, indicating that the goal is to keep crude oil and natural gas prices high.

Also, the decision to "rubleize" trade relations shows that Russia is starting the process of de-dollarization of the world economy, as a result of which currency parities will be determined in the future quite differently than before (in addition to higher gas prices, the problem for the EU is that, in the short, the euro has weakened against the ruble, so its purchasing power for purchasing Russian energy

products is lower). The EU's strong reactions and announcements about giving up Russian energy supplies would make sense if the attempt to politically isolate Russia and break (or at least complicate) its existing relations with non-Western actors had succeeded. In this way, the EU has entered a hybrid war, and it seems that the consequences of the Russian response and the use of energy sources as an unconventional means have been badly assessed.

Because of everything, the current confrontation not only announces, but is also already leaving behind very dramatic outcomes for which the EU is not prepared at all, nor does it show that it has an adequate response.

4. RUSSIA'S COUNTERMEASURES: THE STRATEGY OF LEAVING EUROPE WITHOUT AN ALTERNATIVE

In addition to everything, when observing Russia's countermeasures, it is also noticeable that both foreign and especially security policy are often projected on the basis of energy policy. Much of the Russian setup is similar or identical to the American setup. Put simply – the US wants to use NATO to force the EU to stop buying Russian energy products. Russia's answer is to make NATO completely dysfunctional by stretching the US on several fronts and threatening Europe's energy security. In support of this conclusion, it is necessary to look at the network of alliances and the outbreak of certain armed conflicts in the previous years. Certainly, the outbreak of armed conflicts and the escalation of crises are influenced by a large number of factors. With this analysis, we only want to warn that energy security and energy policy are one of them; it is by no means prejudiced that these are the exclusive or the most important factors.

Map no. 4: Baku – Ceyhan Gas Pipeline and Baku – Supsa Oil Pipeline

The Russian intervention in Georgia in 2008 enabled the essential surveillance over the Baku-Ceyhan gas pipeline, which was supposed to serve as the primary direction for the construction of the 'Nabucco' pipeline (and later for TAP) and the Baku-Supsa oil pipeline (Map no. 4). Support for Bashar Al Assad and direct involvement in the Syrian war prevented the overthrow of the regime in Damascus, the establishment of a new, pro-American (or pro-Western) one, and the design of the Qatar-Turkey gas pipeline. Open support for Marshal Khalifa Belqasim Haftar in the Libyan civil war prevented the victory of the so-called GNA – Government of National Accord, in the creation of which the USA invested. The strengthening of foreign political ties with Egypt, Palestine and Algeria had the effect of making long-term energy security planning of the EU impossible by relying on the Trans-Saharan (Map no. 5) and Eastern Mediterranean (Map no. 6) gas pipelines. The story surrounding both of these projects is complex. In the case of the trans-Saharan connection, it is open to question how it is possible to secure such a long line, bearing in mind the unstable environment and the large number of terrorist or paramilitary formations with opposing political goals in that part of the world. The Russian companies Rosneft, Gazprom and Stroytransgaz are present in Algeria, and since 2010, they have been building new energy capacities and exploring potential deposits of fossil fuels.

Map no. 5: Planned route of the Trans-Saharan pipeline

When it comes to the EastMed project, there is a problem in the demarcation, i.e., conflicting claims of interested parties where their exclusive economic zones are (Egypt, Israel, Turkey, Greece, Jordan, plus Palestine and Cyprus, where there is a territorial problem because of the unrecognized Republic of North Cyprus). It is interesting to look at the historical shift in Russian-Turkish relations from this context, as well as the establishment of the trilateral framework Russia-Turkey-Iran. Turkey is becoming an important distribution hub for the Russian gas (Balkan Stream, whose capacity can be increased in the future by building new lines), but it is also a potential hub for other gas pipelines. As long as Turkey has the capacity to block (together with Egypt and Palestine) the realization of the EastMed gas pipeline, there is no alternative to Russian gas for the EU from this strategic direction.

Finally, there is the escalation of the Ukrainian crisis, which effectively put the EU in an impossible position. By renouncing the Russian energy sources, the EU economy becomes uncompetitive on the global market, which creates social and political tensions with unforeseeable consequences within EU member states. The optimism of Ursula von der Leyen or the European Commission regarding the cessation of purchases of Russian energy products in 2027 or 2030 is one thing, but the reality is quite different. If the trend of buying expensive energy sources (and not a little more expensive, but many times more expensive) continues until 2030, if it lasts eight years continuously, it can completely reshape the European political reality under the pressure of economic hardships and social protests.

Map no. 6: Planned route of the EastMed gas pipeline

Therefore, Russia responded decisively to the USA and, since 2008, has challenged all of its acquisitions in the Caucasus (it was planned for Georgia to join NATO and its stronger presence in Afghanistan), the Middle East (essentially, the development of the situation in Syria represents a defeat for the USA) and North Africa (via Libya, Egypt and Algeria), thus preventing the implementation

of the NATO 2020 Strategic Concept and leaving Europe without alternative supply routes when it comes to natural gas. Also, by establishing completely new relations with Turkey, it resulted in Turkey not following the policy of its Western allies at all since the beginning of the war in Ukraine, and by acting together with Iran, it made Europe aware that an alternative from Iran and its second largest "reservoir" of natural gas in the world, which was difficult to implement anyway (due to the opposition of the USA), no longer exists.

CONCLUSION

It is impossible to plan the EU security policy without ensuring energy security. Stable access to energy sources is the basis for creating economic policy. Considering the importance of the EU for the entire Europe, it is impossible to ensure continental security without the EU's energy security. The thesis that it is necessary to reduce imports and rely on one's own resources has been present in the EU projections for years. However, little has been done in this regard. Ever since the end of the 1960s, the connections with the Russian (Soviet) energy sector have had the effect that, over the decades, the dependence of European consumers on Russian producers has become greater. Only since 2010, and thanks to the USA, which used NATO, did the creation of new strategies begin to reduce the EU's dependence on Russian energy sources.

However, with its political actions and military interventions, Russia prevented these strategies from being implemented. Europe's security still depends on Russian energy, and little can change in that respect, regardless the announcements by EU officials that a different scenario is possible by 2027 or 2030. Even contrary to those claims, following current trends and the high degree of success of the Russian political action and military interventions, it should not be ruled out that new crises or new wars will follow, if by continuing the current US strategy (using NATO) some new scenarios of "energy separation" of the EU from Russia are attempted. Viewed from that angle, the escalation of the Ukrainian crisis may not be the last of such nature in Europe.

REFERENCES

1. Bariš, Katinka. 2009. *Cevovodi, politika i moć: budućnost energetskih odnosa EU – Rusija*. Beograd: Evropski pokret u Srbiji.
2. Buchholz, Katarina. 2022. Which European Countries Depend on Russian Gas?. *Forbes*. https://www.forbes.com.
3. Buffet, Laura. 2016. Europe increasingly dependent on risky oil imports. *Transport&Environment*. https://www.transportenvironment.org.
4. Bushuev, V. V., Troitskii, A. A. 2007. The Energy Strategy of Russia until 2020 and real life. What is next? *Thermal Engineering*, (54): 1–7.
5. Carlisle, Tamsin. 2009. Qatar seeks gas pipeline to Turkey. *The National*. https://www.thenational.ae.
6. Đukić, Srećko. 2009. *Vreme energije: više od diplomatije*. Beograd: Službeni glasnik.
7. European Commission. 2022. EU sanctions against Russia following the invasion of Ukraine. https://eu-solidarity-ukraine.ec.europa.eu.
8. European Commission. 2007. Lisbon Treaty. Brussels: European Commission. http://europa.eu.
9. Eurostat. 2020. EU imports of energy products – current development. https://ec.europa.eu
10. Kliesen, Kevin L. 2001. Rising Oil Prices and Economic Turmoil: Must They Always Go Hand in Hand? St. Louis: Federal Reserve Bank of St. Louis. https://www.stlouisfed.org.
11. NATO. 2010. NATO 2020: Assured Security; Dynamic Engagement. Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO. http://www.nato.int.

12. NATO. 2008. Bucharest Summit Declaration Issued by the Heads of State and Government Participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008.

13. NATO. 1949. The North Atlantic Treaty. Washington: NATO.

14. Pirani, Simon. 2007. *Ukraine's Gas Sector*. Oxford: Oxford Institute for Energy Studies.

15. Proroković, Dušan. 2018. Reaktualizacija koncepta Međumorja (Intermarijuma) i položaj Srbije. In: Dušan Proroković, Vladimir Trapara (eds.), *Srbija i svet u 2017. godini*. Beograd: Institut za međunarodnu i privredu: 51–67.

16. Proroković, Dušan. 2019. Energetska bezbednost SAD i spoljnopolitičko pozicioniranje Srbije. In: Dušan Proroković (Ed.), *Energetska diplomatija Republike Srbije u savremenim međunarodnim odnosima*. Beograd: Institut za međunarodnu politiku i privredu: 114–134.

17. Proroković, Dušan & Perović, Milorad. 2013. Strateški koridori i cevovodi i njihov uticaj na geoekonomski položaj balkanskih država. *Nacionalni interes,* X (18): 105–133.

18. Smith, Cristopher. 2011) Nord Stream natural gas pipeline begins line fill. *Oil & Gas Journal*. https://www.ogj.com.

19. Smith, Keith C. 2010. *Russia-Europe Energy Relations Implications for U.S. Policy*. Washington D.C.: Center for Strategic & International Studies.

20. Turksen, Umut. 2020. *EU Energy Relations with Russia. Solidarity and the Rule of Law.* London: Routledge.

PART TWO: CRITICAL INFRASTRUCTURE PROTECTION

Gjorgji Alceski Ph.D.*)
Sasho Shterjov**)

UDC: 351.78:[616.98:578.834-036.21(100)
351.78:656.7

APPROACH TO THE REALIZATION OF SECURITY MEASURES OF CRITICAL INFRASTRUCTURES IN CONDITIONS OF PANDEMICS AND DURING IMPLEMENTATION OF SAFETY PROTOCOLS

Abstract: *All complex security situations which we face and during which arises the need for introducing prompt and adequate preventive measures and deal with the resulting crisis, undoubtedly require a complex approach, in which implementation of security measures should follow the measures and safety protocols. This complexity observed through the prism of providing security to critical infrastructures is in direct relation to the problems, difficulties and dilemmas faced by safety experts.*

Having in mind the relevant knowledge about the complexity of dealing with the pandemic caused by the Covid-19 virus and the fact that a large number of critical infrastructures, including the transport sector, faced serious challenges, we will see that the factors that lead to the inefficiency of the security should be timely resolved in order to prevent such occurrences and enable improvement in continuity.

The necessity of recognition, combat and post-crisis recovery from all types of threats of the contemporary times is an obligation of all involved entities in security and safety, and these processes should therefore function flawlessly and be maximally coordinated in the accepted and established system of each state.

Hence, this paper will aim to examine and analyze the new security challenges, including pandemics as one of the more structural threats, as well as their impact on the new security threats. A concrete contribution will also be given both in the general and theoretical aspect of this area, depicted in the form of presentation of practical aspects of applying the methodology of the security and safety systems. Through a scientific scope of view, in which the applicability of advanced procedures and technologies implemented in the development of security and safety are supposed to respond to more dilemmas in the segments of planning, functionality of security services in conditions of pandemics, coordination, exchange and selection of information, applicability of advanced technologies should be put to the service of creating a stable security system and strengthening the safety facilities of critical infrastructures.

Key words: *critical infrastructures, security, safety protocols, pandemic, measures.*

*) Airport Director at Ohrid St. Paul the Apostle Airport in TAV Macedonia and University Professor at the Faculty of Philosophy of the University Ss. Cyril and Methodius in Skopje, researcher at the Institute for Security, Defense and Peace studies.
**) Safety Manager – TAV Macedonia.

1. CHALLENGES TOWARDS THE IMPLEMENTATION OF SECURITY OF THE CRITICAL INFRASTRUCTURES

Each sector of critical infrastructure has its unique characteristics, operating models, and risk profiles, which have institutional significance and specialized expertise related to that sector (The White House, Office of the Press Secretary 12 February 2013). Given the large number of critical infrastructures, significant challenges and difficulties arise upon their protection. Analyzing the enormous negative consequences caused by the *Covid-19* pandemic, which resulted in a catastrophic decline in economy, states, including operators of critical infrastructures in coordination with public health authorities, called for implementation of a set of measures aimed at reducing health risks on one hand, and continuing the basic business activity on the other. The goal was to contribute to an efficient, safe, and sustainable process of operation and return to the "new normal" operation.

As an illustration, let's start by examining the negative economic consequences of the *Covid-19* pandemic through the lens of the airline industry. The impact of the coronavirus (*Covid-19*) pandemic on global air transport is without precedent. For the year 2020, global passenger numbers fell by 60 per cent or to 2.7 billion, compared to 4.5 billion in 2019, that is, 74 per cent in international traffic and 50 per cent in domestic traffic. Airlines have seen a 66 per cent decline in revenue passenger kilometres, and airport passenger numbers were down 57 per cent in 2020. The traffic decline was estimated to have resulted in revenue losses amounting to USD 371 billion and USD 112 billion for airlines and airports, respectively. The World Tourism Organization (UN WTO) also estimated a loss of USD 1.3 trillion in export revenues from tourism. With the *Covid-19* pandemic accelerating across the globe, headwinds to air transport remain particularly pronounced in 2021. The updated ICAO projections indicate that world scheduled passenger traffic for the first half of 2021 will be reduc d by 59-66 per cent (1.3-1.4 billion), compared to 2019 levels (Council Aviation Recovery Task Force, 10 March 2021; ICAO, n.d.).

Therefore, the dangers that follow modern, contemporary society through the prism of the critical infrastructures require a permanent, expert and professional countering threats, implementation of measures and activities directed towards strengthening the security capacities of the state, including private and corporate security[30)] as an integral segment in the national security system. On the other hand, when it comes to the safety of vital facilities – critical infrastructure and the consequences of their non-functionality, the need undoubtedly emerges for a special concept of a systemic approach to developing security/safety, especially amid crises.

Based on the overall analysis of the concept and term "critical infrastructure", considered through the prism of security and the offered indicative lists for critical infrastructures from the West, and guided, above all, by the guidelines given by the European Union[31)], we can conclude as follows: *Critical infrastructure represents facilities, devices, installations, products, services and all systems that are in direct or indirect connection with the normal functioning of the state so that their failure would cause serious consequences on national security, economy, health, the functionality of the state apparatus, social or other type of consequences* (Алчески 2016; Алчески, Тунтев 2021).

The responsibility for the protection of the national critical infrastructures mainly belongs to the operators of the critical infrastructures. Hence, analyzing the wide spectrum of threats from both the safety and the security aspect makes security very complex, just because of the balance of measures and work procedures that, in some cases, diverge.

---

30) See more in: Бакрески, О., Триван Д., Митевски, С. 2012. *Корпорациски безбедносен систем.* Скопје: Комора на Република Македонија за обезбедување на лица и имот and Кековић, З., Димитријевић, И. Р., Н. Шекарић. 2018. *Корпоративна безбедност: хрестоматија.* Београд: Универзитет у Београду, Факултет безбедности.

31) On the topic of EU guidelines, see more in: The Council of the European Union. 23 December 2008. "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". *Official Journal of the European Union.* https://eur-lex.europa.eu as well as: Commission of the European Communities. 17 November 2005. "GREEN PAPER ON A EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION". Brussels: Commission of the European Communities.

The analysis made by many relevant scientific and professional organizations clarifies that the implementation of modern systems and procedures in development of the security and safeguarding of critical infrastructures is a necessity and a process that should have its own continuity towards the creation of the desired security climate, with the full implementation of safety protocols.

In many countries, a significant part of critical infrastructures is privately owned, and therefore, there must be cooperation with state institutions. In Germany, four fifths of the critical infrastructure is private (Federal Ministry of the Interior and Community n.d.). In the US, about 85% of critical infrastructure is privately owned as well, but the reality is that market forces alone are not enough to drive the necessary investment in protection (Aureswald, Branscomb, La Porte & Michel-Kerjan 2005, 77). As a result, experts describe the EU's work on critical infrastructure protection as assisting countries within clearly defined sectors, with appropriate coordination between sectors (Larsson 2007, 9-24). The issue of cooperation between the EU and the member states in the process of protecting the critical infrastructure can be the stance of some states that certain data must be preserved within national frameworks (Jarlsvik & Castenfors 2004, 64).

If we look at the need to protect critical infrastructure in the US, through risk management we will see that it is very broad and made up of partnerships between owners and operators; federal, state, local and territorial governments; regional entities; non-profit organizations; the academia, etc. Managing the risks of serious threats and the dangers associated with physical and cyber threats to critical infrastructure requires an integrated approach in terms of the following:

- "Identifying, preventing, detecting, and preparing for threats and dangers to critical infrastructure;
- Reducing the vulnerability of critical assets, systems and networks; and
- Mitigating the possible consequences of incidents or negative events that occur on critical infrastructures" (Homeland Security 2013).

The success of this integrated approach depends on the full range of capabilities, expertise and experiences in the infrastructures and associated stakeholders (Homeland Security 2013, 7).

2. THE NEED FOR BALANCE BETWEEN SAFETY AND SECURITY AMID PANDEMIC THROUGH THE PRISM OF AIR TRAFFIC

It is extremely important that to determine the process of securing and safeguarding critical infrastructures design it in order to be efficient in dealing with new risks and dangers as one of the key prerequisites, or pre-requirements, for proper functioning of security.

Airports, together with the national authorities, organize protocols for better coordination and protection related measures[32)]. The plans that refer to this issue include several aspects, such as the following: communication and exchange of information with the public, observation and monitoring of the situation, logistics in accepting and transporting passengers to health organizations, use of appropriate protective equipment, access control to and from airports, coordination with local and national health organizations, etc. Responsibility for managing the risk of infectious diseases at airports rests primarily with the local, regional and national public health authorities, as well as the relevant airport operator. Therefore, the communication and sharing of information with internal and external airport entities, as well as with the passengers, regarding the travel protocols and restrictions, must be consistently applied.

Following the example of aviation and airport security, as one of the more regulated areas when it comes to protection and security, and as one of the areas most affected by the pandemic, security protocols have been implemented with the application of appropriate protective measures and activities.

[32)] See more in: Airports Council International. 24 January, 2020. "Transmission of Communicable Diseases". ACI Advisory Bulletin. https://aci.aero.

Image 1 – Safety vs security measures

Historically, security measures and the implementation of modern security systems have been in constant growth and improvement. However, changing health requirements in aviation and airport operations have made them face a new challenge. First of all, the regulatory requirements were implemented in terms of changing the procedures through operational directives, maintaining the standards for the provision and implementation of the health protocols.

The vision and mission depend on the achievement of the goals, which represent the strategic direction towards which the critical infrastructures should focus:

– Rapid capacities restructuring based on new risks,

– Implementation of measures and protocols,

– Introduction of compatible technologies and systems,

– Permanent education according to new challenges.

2.1. CAPACITIES RESTRUCTURING AND IMPLEMENTATION OF MEASURES AND PROTOCOLS

In terms of *capacity restructuring*, numerous factors apply, including public health authorities' guidance (led by travel risk levels), government travel restrictions and requirements, airline and airport operational capacity, etc. Phases were developed, starting from limited travel with minimal movement, which

revolved into initial increase in travel as the next phase, with relatively low passenger volumes, allowing airlines and airports to introduce aviation public health practices appropriate to the volume of passengers and the presented risk. Following the medical criteria and the applicability of the measures, the volume of passengers continued to increase. Furthermore, with the reduction of the national level of health alert, risk mitigation measures continue to be reduced, modified, or terminated.

In terms of *risk mitigation*, *measures and protocols* are considered through the following:

- **The airport module** contains specific elements to address guidelines for airport terminal building, cleaning, disinfection, hygiene, physical distancing, personnel protection, access, area inspection, security screening, airside area organization, passenger transfer, movement and passenger transportation, baggage handling and control in the arrival areas, etc.
- **The aircraft module** contains specific instructions relating to boarding processes, seating arrangements, hand baggage accommodation, interaction in the aircraft, passenger cabin organization, food and beverage services, toilet access, crew protection, management of sick passengers or crew members and cleaning and disinfection of the interior of the aircraft, the cargo area, etc.
- **The crew module** contains guidelines for safe and sustainable travel closely coordinated according to international protocols in the direction of the approach to treatment, in accordance with prescribed public health standards. The crew module also contains specific instructions for contacting a crew member with a suspected or positive case of *Covid-19*, practices when symptoms appear, etc.
- **Cargo** flight crews apply the same health and safety considerations as passenger flight crews. This section addresses to aviation public health, including physical distancing, personal sanitation, protective barriers for transfer points to the ramp and loading and unloading, and other mitigation procedures (Council Aviation Recovery Task Force 10 March 2021).

It must be noted that, when it comes to security personnel, who are basically one of the most exposed to risk, many protective measures and equipment, such as disposable gloves, surgical masks, hats or medical caps, goggles, and protective suits, were implemented; furthermore, it was defined that hands should be disinfected before wearing personal protective equipment. All this further complicated the process of screening and searches, which should be carried out in accordance with international standards for security against acts of unlawful interference.

2.2. INTRODUCTION OF COMPATIBLE TECHNOLOGIES AND SYSTEMS AS SUPPORT IN THE IMPLEMENTATION OF SECURITY

Security systems are constantly developing. In order to satisfy the requirements arising from practice amid pandemics, implementation of modern systems should depend on several factors; moreover, it is important that the justification to invest in equipment and resources/supplies safety-wise should be constant, and depending on the needs and necessities of the given moment. Along with technological development, both operational and spatial considerations are the key drivers in the evolution of security checkpoints. Considerable efforts have been made to satisfy the control process and achieve the right balance of security in coordination with the necessary protective measures.

We have also witnessed many cases of automation of processes, depicted in self-service module implementation, directed towards ensuring health-related safety. For this purpose, contactless technology was introduced in order to reduce the risk of transmission, though it, in some cases, complicated the work of security services. However, in order to facilitate and promote the best practices for slowing the spread of *Covid-19*, we have witnessed introduction of displays that inform the public about the measures that should be taken. Preparation and clear directions are the initial prerequisite for further processes.

In this direction, CT scanners have proven to be a very effective system for passenger control, cabin baggage and heavy baggage, which brought multiple benefits, such as increasing the throughput of the security lane, facilitating the lifting of LAG (liquid, aerosol and gel) restrictions and removal of the need for passengers to unpack electronics and similar items, and at the same time avoid physical contact or ensure minimal distance because, first and foremost, security screening employees need to be safe while performing their job duties.

For this purpose, security systems, which, in addition to the well-known functions of a security related character, also perform contactless measurement of body temperature, etc., are becoming more and more desirable. These systems serve to screen personnel using the "face recognition" method, and often contain a thermometer. With this method, a contactless measurement of body temperature can be carried out, thus limiting the access of persons with an increased body temperature, and at the same time alerting the authorities of a possible case of infection. In this context, it is necessary to mention that walk-through metal detectors are also used to measure body temperature. This provides one more check before the passengers move from one zone to another, and also protects the security screening staff in case they have to use a manual screening method.[33)]

Following the development of technology that has been observed in recent years, and based on the needs of increasing protection, additional innovative systems have been developed for the detection of even the smallest objects that pose a threat and that are owned by the person. The technology that has the possibility to detect traces of explosive devices (ETD), millimeter radiation or MMW (Millimeter-Wave) with a radiation length between 1mm and 10mm (enough to penetrate through fabric and enable resolution), is also often used[34)].

[33)] See more in: Polimek. 2020. POLIMEK ELEKTRONIK SANAYI VE TICARET A.S. Izmir, Turkey: Polimek. https://www.polimek.com.tr.

[34)] See more in: Airports Council International. 20 March, 2020. "Security screening best practices during COVID-19". Advisory Bulletins. https://aci.aero.

Namely, primarily, we are stressing the importance of implementation of security screening for the safety of passengers and staff, minimization of contacts, active use of the ETD, one-time use of equipment and resources/supplies, full and consistent application of SMS, development of procedures and processes in case of positive cases, introduction of alternative lines of movement and access control, as well as full following and observance of recommendations by international aviation organizations such as: ICAO – International Civil Aviation Organization, ACI – Airports Council International, ECAC – European Civil Aviation Conference, EASA – European Aviation Safety Agency, IATA – International Air Transport Association, etc.

Also, biometric verification technology may be the right answer, which needs to be implemented as a replacement for physical aids. Nowadays, an increasing number of airports, as well as companies with serious risks, are turning to positive identification with the help of biometric models to confirm identity and accurately represent which person is trying to gain access to a certain restricted area. Biometrics refers to parameters related to human characteristics. Biometric applications involve taking a sample of individuals which is then digitized, automated, and made unique in a database. The use of biometric data identifies the person who gains access to the restricted area. Access to the restricted area can only be given to a part of the staff, to those who have specific work duties. These systems can also respond to very delicate matters related to danger cases. For example, in case of an evacuation, the number of people and personnel who were present in the threatened area will be known exactly. As the most suitable system for contactless access control, we should stress as follows:

– *Facial biometrics*, where individuals are identified by analyzing the features of their face, which cannot be easily changed, given that they are projected by analyzing the distance between certain points on the face. Facial images are taken using photos and videos and then shared. The facial biometrics represents a unique biometric technology used for verification, identification, and surveillance purposes.

- *Iris* – this technology measures the unique features of the iris, the colored ring around the pupil that contains approximately several hundred different features and represents a rich source of biometric data.
- *Voice* – The voice recognition system captures parts of a person's speech, who must speak into a microphone and repeat parts of phrases. A sample of their voice is saved for future comparisons.

Of course, these access control systems need to be supplemented with an appropriate monitoring system that will be under constant supervision by the operators.

With the use of a CCTV system, the percentage of intrusion detection and control over automatic access control systems is greatly increased, especially when it is used to confirm alarms from other security systems. However, the effectiveness of the systems will primarily depend on the selection of appropriate equipment and the methods of equipment installation.

There is no doubt that equipping the security services in accordance with modern achievements in this area implies the possibility of unhindered performance of the assigned tasks, adequate to the risks and dangers accompanying the pandemic.

2.3 EDUCATION AND DEVELOPMENT OF SECURITY AWARENESS

Constant education in accordance with the new challenges, as well as security awareness, are some of the most important factors for overall protection, with the ultimate goal of preserving human lives and material goods.[35)] In order to achieve an adequate company security policy, every single employee, regardless of the job position and professional profile, needs to have elementary knowledge of security, especially for the duration of his work duties. The worker needs to be careful and inform about any suspicious or abnormal situation. Security awareness also implies

[35)] See more in: Џонс, Г., Џорџ, Џ. 2008. *Современ менаџмент*. Скопје: Глобал комуникации.

compliance with the security/safety regulations that apply to all employees in the company, but it also implies response in certain specific situations where you need to show decisiveness and determination in case when it is necessary to solve a certain situation correctly, whether in regular conditions or in case of an emergency.

Amidst pandemic, it is obvious that the approach to developing awareness needs to be multi-faceted. To this extent, we hereby present the approaches regarding personnel, passenger management and facilities.

Personnel: Education of the staff in order to familiarize themselves with the latest information about the pandemic through the use of health care related talks and discussions, advice, circular letters sent via e-mail, management of stressful situations, continuous online trainings is pivotal, paired with monitoring the health of airport staff by encouraging constant monitoring of possible symptoms among employees and developing self-isolation awareness; limitation of access, especially to vital rooms and reduction of presence, i.e. separation, as well as provision of backup teams if any of the employees are in quarantine, etc. should be implemented as well; introduction of physical distance at the workplace where staff are present, etc, is one of the most significant measures.

Passenger management: Temperature screening and health declaration according to regulations, hygiene and disinfection, physical distance for passengers in all areas of the airport, information for passengers – posters and informational displays about the necessary procedures, etc. present some of the most significant measures.

Facilities: Organization of facilities in the context of entrances and exits, identification of critical rooms and their maintenance, food and restaurant services to be organized in accordance with health protocols, disinfection of public areas, equipment and supplies, adjustment of ambient air temperature and increasing ventilation, etc. all represent recommended measures.[36)]

[36)] See more in: Airports Council International. 2020. *Airport Operational Practice: Examples for Managing COVID-19.* https://store.aci.aero.

In general, security is everyone's responsibility! "Promoting an effective security culture is crucial to achieving good security results. A strong security culture must be developed from top management through and within every organization. The existence of a well-trained, motivated and professional workforce is a key prerequisite for effective security in aviation" (ICAO n.d.).

Security culture is a set of norms, beliefs, values, attitudes and assumptions that are inherent in the daily operation of an organization and are reflected by the actions and behavior of all entities and personnel within the organization.

The benefits of an effective security culture include:

- Employees take responsibility for security issues,
- Levels of compliance with protective security measures are increasing,
- The risk of security incidents and disturbances is reduced by employees thinking and acting in more security ways,
- Employees are more likely to identify and report behavior/activities that concern them,
- Employees feel a greater sense of security; and
- Security is improved without the need for large costs (ICAO n.d.).

A contribution to general security can be given by every single employee engaged in the company, regardless of their job position according to the organizational structure. Developing such an awareness is an ongoing process, that is, it includes changing the awareness of the staff in relation to safety and the dangers to which the staff and the institution may be exposed.

CONCLUSION

New forms of threat, arising from the latest developments related to the coronavirus pandemic that has caused a global health and economic crisis, as well as the Russian attack on Ukraine this year, point to the fact that we are entering an era in which we will face new economic, health, social and security challenges and in response to which we must implement all the latest crisis management modalities.

Designing a company's safety system in the context of a pandemic is an activity that consists of several characters, from the initial basis and the answer to the question of what it is that we are protecting, then what are the threats, risks and dangers, their type and character, up to the implementation of the concept for security and implementation of protective protocols and measures. For those reasons, every bigger company that has a strategic interest of the state or is declared as a critical infrastructure needs to develop management plans in crisis and post-crisis recovery through the development of modalities for rapid restructuring of capacities based on new risks, implementation of measures and protocols, introduction of compatible technologies and systems, permanent education according to new challenges, etc.

That synergy between safety, which is basically a state in which dangers, threats and risks are annulled or reduced and controlled to an acceptable level, and security, which includes all specific measures and activities in the fight against acts of illegal behavior, needs to be balanced. Based on positive practices from a large number of countries, management needs to be focused on understanding all aspects – organizational, regulatory, structural, essential, technical, etc., with a tendency to offer certain universal and practical solutions that would improve and advance the existing security system in crisis conditions.

The fact that the possibility of carrying out illegal actions against critical infrastructures aimed at intentional destruction through consciously performed acts of unlawful interference is not excluded in the conditions of a pandemic crisis, it is necessary for the security apparatus to be set at the highest level through appropriate methodologies for the realization of the physical, operational – technical and cyber security (Stallings 2017).

New threats require the inclusion of advanced security systems that follow modern new technologies and advances in security. It is precisely the development and application of advanced security equipment in the function of providing the critical infrastructure that will undoubtedly contribute to the inclusion of new models of security devices, supplies/resources, and equipment, with the help of which it will be easier to determine, i.e., to find certain illegal substances or objects that threaten security of people and material goods. The training system, starting from security awareness (security/safety culture) as a significant factor for overall safety and an adequate safety policy of education based on job specificities and risks, is one of the keys of the success of any modern company.

REFERENCES

1. Airports Council International. 2020. *Airport Operational Practice: Examples for Managing COVID-19*. https://store.aci.aero.
2. Airports Council International. 20 March, 2020. "Security screening best practices during COVID-19". Advisory Bulletins. https://aci.aero.
3. Airports Council International. 24 January, 2020. "Transmission of Communicable Diseases". ACI Advisory Bulletin. https://aci.aero.
4. Aureswald, P., Branscomb L. M., La Porte T. M. & E. Michel-Kerjan. 2005. The Challenge of Protecting Critical Infrastructure. *Issues in Science and Technology*. Vol. XXII, No. 1, Fall 2005. Arizona State University.
5. Commission of the European Communities. 17 November 2005. "GREEN PAPER ON A EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION". Brussels: Commission of the European Communities.
6. Council Aviation Recovery Task Force. 10 March 2021. "Take-off: Guidance for Air Travel through the COVID-19 Public Health Crisis". Montreal, Canada: International Civil Aviation Organization. https://www.icao.int.
7. Federal Ministry of the Interior and Community. n.d. "Critical Infrastructure Protection". https://www.bmi.bund.de.
8. Homeland Security. 2013. *NIPP 2013: Partnering for Critical Infrastructure: Security and Resilience.* US: Homeland Security.
9. ICAO. n.d. "Economic Impacts of COVID-19 on Civil Aviation". https://www.icao.int.
10. Jarlsvik, H., Castenfors, K. 2004. Säkerhet och beredskap i Europeiska unionen [*Security and Preparedness in the EU*]. Stockholm: Krisberedskapsmyndigheten.
11. Larsson, R. 2007. *Tackling Dependency: The EU and its Security Challenges*. Swedish Defense Research Agency.

12. Polimek. 2020. POLIMEK ELEKTRONIK SANAYI VE TICARET A.S. Izmir, Turkey: Polimek. https://www.polimek.com.tr.

13. Stallings, W. 2017. *Cryptography and Network Security: Principles and Practice.* Seventh Edition. Pearson, Global Edition.

14. The Council of the European Union. 23 December 2008. "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".*Official Journal of the European Union*. https://eur-lex.europa.eu.

15. The White House, Office of the Press Secretary. 12 February, 2013. "Presidential Policy Directive – Critical Infrastructure Security and Resilience". https://obamawhitehouse.archives.gov.

16. Алчески Ѓ. 2016. Имплементација на современите безбедносни системи и процедури во развој на обезбедување на виталните објекти за Република Македонија (со осврт на аеродромската безбедност). Doctoral Dissertation.

17. Алчески, Ѓ., Тунтев, Т. 2021. *Аеродромите како критична инфраструктура.* Скопје: Комора на Република Македонија за приватно обезбедување на лица и имот.

18. Бакрески, О., Триван Д., Митевски, С. 2012. *Корпорациски безбедносен систем.* Скопје: Комора на Република Македонија за обезбедување на лица и имот.

19. Кековић, З., Димитријевић, И. Р., Н. Шекарић. 2018. *Корпоративна безбедност: хрестоматија.* Београд: Универзитет у Београду, Факултет безбедности.

20. Џонс, Г., Џорџ, Џ. 2008. *Современ менаџмент*. Скопје: Глобал комуникации.

Ćurčić Milica*)

Nikola Zdolšek**)

Gvozden Tasić***)

UDC: 351.78:[623.45:005.334

CRITICAL INFRASTRUCTURE PROTECTION AGAINST CBRN THREATS

Abstract: *CBRN security has a high priority for the nation's Critical Infrastructure Protection. Comprehensive protection against CBRN threats includes a complex analysis of many aspects of CBRN threats, vulnerabilities, response plans, programs, procedures and protocols, communication infrastructure, personnel, legal and economic factors. The paper provides an overview of different approaches to the protection of national critical infrastructure against CBRN threats. Those approaches take into account specifics arising from the main properties of used CBRN agents - toxicity, latency, persistency, and, transmissibility. In this research, a qualitative research model was used to incorporate knowledge from different scientific disciplines: security science, physical chemistry, environmental protection and law. Achieving the research objective required the use of different methods: literature review, qualitative content analysis, and scenario methods. In that way, a concrete contribution is made to the analysis of existing security and safety procedures and its further development.*

Key words*: Critical Infrastructure, CBRN Threats, Security, Protection, First Responders.*

*) PhD candidate, Vinča Institute of Nuclear Sciences – National Institute of Republic of Serbia, University of Belgrade, Belgrade, Serbia.

**) PhD, Vinča Institute of Nuclear Sciences – National Institute of Republic of Serbia, University of Belgrade, Belgrade, Serbia.

***) PhD, Vinča Institute of Nuclear Sciences – National Institute of Republic of Serbia, University of Belgrade, Belgrade, Serbia.

INTRODUCTION

In recent years, CBRN materials become a weapon of choice for numerous attacks, targeting individuals, civilians as well as a different object, including critical infrastructure. In addition to perpetrators' potential to use this type of weapon to achieve its goals, the probability of CBRN accidents has increased due to the process of globalization and technological progress. Numerous types of CBRN materials are now more available and widely used as radioactive sources, and the spread of nuclear facilities and chemical industry, medical and biological laboratories occurs. This increases the probability to CBRN agents becoming available to potential perpetrators of attacks on critical infrastructure, but also increases the probability of technical-technological accidents, which could indirectly threaten critical infrastructure objects. Risk assessment shows that CBRN threats are considered as low probability, but with high impact risks. Any incident involving CBRN materials, whether it is deliberate or accidental, can potentially cause life losses, harm the public's health, disrupt society functioning, contaminate the environment, and, consequently, damage a state's economy. Even at a small scale, a CBRN attack results in significant and lasting disruption, widespread fear and uncertainty. The scale and nature of CBRN attacks vary and therefore require diverse response procedures, ranging from relatively simple countermeasures to more complex mitigation actions. For an adequate response, cross-sector cooperation is the base of a low number of casualties and fast localization of the threat sources.

Critical infrastructure protection is one of the priorities of each state and it represents the basis for maintaining the functionality of the social community in emergencies. It includes systems, networks, and facilities of national importance which disruption may have serious impacts on national security, health, property, environment, security, and economic stability. The main goal of critical

infrastructure protection is to provide reliability, high performance, continuous operation, safety, maintenance, and physical and cyber protection. States intend to identify and analyze critical sectors, sub-sectors, processes, and objects using different methodological and political approaches. In the process of defining the critical infrastructure protection policy through prioritizing which assets of infrastructure are most essential to its function, the biggest problem for states is the incredible complexity of infrastructure systems. Furthermore, there is a large number of infrastructure sectors that simultaneously include numerous subsections, branches of industry, services, and production areas and have a specific vertical structure. This indicates an increasingly strong interconnection of critical infrastructures, but also the danger of identifying all infrastructures as critical due to unclear boundaries between critical and non-critical infrastructure.

In literature and national regulations, we can find various classifications of critical infrastructure objects. Different definition and approaches to understanding critical infrastructure classification includes the following objects: food, water, agriculture, health services, emergency services, energy (electrical, nuclear, gas and oil, dams), traffic (air, road, rail, ports, waterways), information and telecommunications, banking and finance, chemical plants, defense industry, mail and distribution of goods, national monuments and other cultural values (Mićović 2020, 10).

An alternative approach advocated by some experts (Moteff, Parfomak 2004, 14) maintains that numerous risks, threats and vulnerabilities should be identified before moving on to identifying critical infrastructure. Rather, support and maintenance of a database of vulnerabilities should be integrated with threat analyses. That approach will be applied in this paper through analysis of a specific threat that is transforming very fast in combination of used agents, but still stay similar in characteristic, CBRN threats.

1. THE MAIN PERPETRATORS OF CBRN THREATS

In comparison to other security threats, one of the main specifics of CBRN attacks is the fact that perpetrators need to have specific knowledge, expertise, and skills. The complexity of CBRN threats makes it unlikely that those kinds of attacks could be accomplished by a single person. Rather, those attacks are conducted by a group that includes a number of people with different tasks: leaders, financiers, suppliers of CBRN agents, bomb builders, drivers, executors of attack/those who plant the CBRN weapons, triggermen, and people who exploit the attack. The threat emerges from both state and non-state actors, with different motivations.

The CBRN threat can emerge from state actors that use CBRN agents against other state, non-state actors and individuals, or from accidents during storage, transport, training, testing, developing and demolition. Although the possibility of the state carrying out a CBRN attack is not excluded, we can find fewer examples and analyzes in the literature. These potentials are mostly associated with non-democratic regimes, failed states, or from rouge state trade. Some of the examples are situations in which armies uses CBRN agents as a part of military operations; states might use CBRN agents in civil war, state actors use CBRN agents in assassinations or state sells those agents to other states or non-states actors. In the EU, the main concern regarding state actors is related to the weakening of the international regimes against CBRN weapons. The second issue mentioned is an assessment of the CBRN risk presented six countries of concern, namely Russia, Iran, North Korea, Syria, Turkey and Saudi Arabia (Rimpler-Schmid et al. 2021, 38).

It was estimated that the main perpetrators of these threats are likely to be non-state actors, with a different motivation and capacity to develop and use CBRN agents. Ideology plays a decisive role in a group's objectives and modus operandi, because the use of CBRN weapons may or may not be appropriate for

their ideological agenda, or encompasses their overall and specific operational objectives. Six types of groups have been identified as potential CBRN weapons users that may increasingly be able to acquire relevant CBRN weapons-related knowledge, skills and possibly materials. These include nationalist, separatist or irredentist groups; radical religious fundamentalist groups; apocalyptic or millenarian "new religious movement" groups; single-issue groups; right-wing groups; and social revolutionary or secular left-wing groups (Meulenbelt and Nieuwenhuizen 2015, 831-840).

For the last 20 years, the world has been in constant fear of terrorist attacks as the biggest global security threat. This fear was further increased by the very thought that terrorists could attack it by means of a destructive means, such as a CBRN agent. In 2017, the EU established the Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks, which stresses that the EU is currently facing a range of terrorist threats and attacks of a violent nature, which have sought to carry out mass-casualty attacks in the EU with the aim of maximizing both the number of victims and the psychological and economic impact on society (European Commission, 2017, 2). According to this Plan, terrorist organization haven't already used CBRN agents in Europe, but there are credible indications suggesting that they might have the intention of acquiring CBRN materials and developing the knowledge and capacity to use them.

In addition to other perpetrators of CBRN attacks, in literature we can find rogue scientists due to the potential availability of these materials to them and the specific knowledge they possess. There are major concerns that former weapons scientists or experts who have the ability either to aerosolize biological agents properly or to activate radiological or nuclear devices may be recruited by non-state actors. Then, organized crime group that can be involved in the procurement and transport of CBRN materials are also mentioned as potential perpetrators. However, it is more likely that these actors would be a part of an organized group that carries out one phase of the attack, rather than being the final perpetrators of the attack.

Meulenbelt and Nieuwenhuizen graphically presented the several steps of the development, use, and consequences of CBRN agents in chronological order (Figure 1). This kind of methodology is very interesting for comparison with other authors who research this scientific subject. They started with the investigation of factors that motivate actors to employ CBRN weapons, which is an approach commonly found in research presented by other authors.

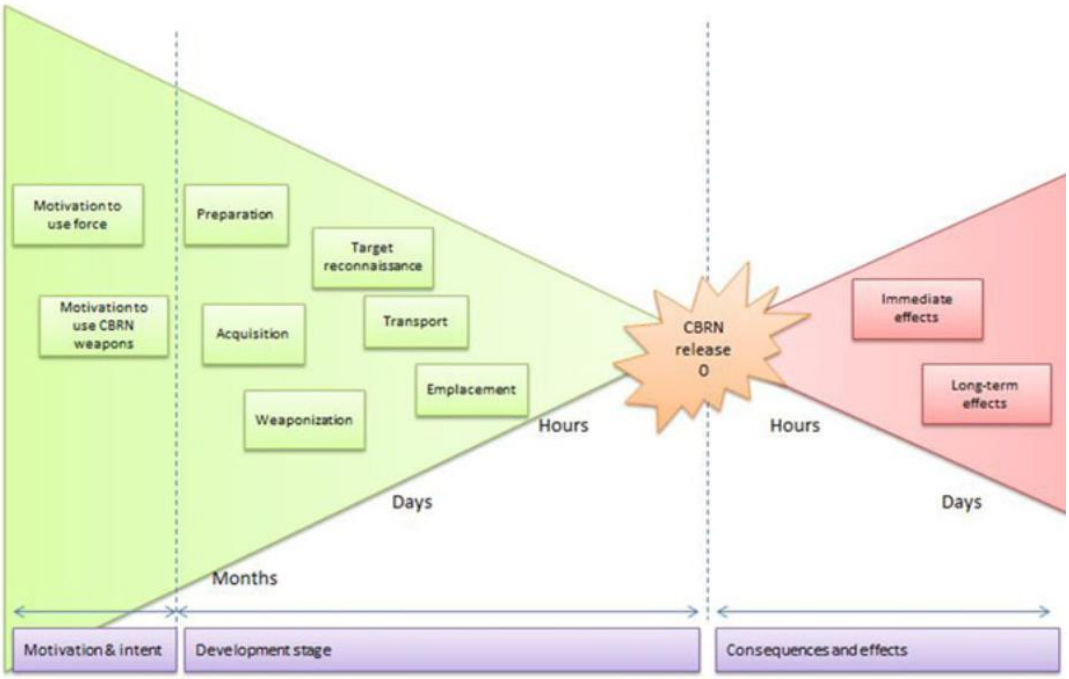


Figure 1 – Overview of the various elements of the threat and the stages of the process, from the formation of motivation and intent, to the actual completion and triggering of a CBRN weapon, as well as the impact of a CBRN attack (Meulenbelt, Nieuwenhuizen 2015, 833)

The majority of authors begin their analysis by identifying potential actors who would be ready to use this means, characteristics of those groups, goals that perpetrators are trying to achieve, etc. Mostly, they represent a different type of non-state actors, among which terrorists are the most often recognized. The next question that emerges is why the perpetrator of the CBRN attack chooses this particular weapon among the mass of other possibilities. We can find that terrorists

seek to use CBRN agents as an adequate means that can produce or inflict mass casualties and create mass panic. A review of the potential implications of CBRN and past incidents shows common findings on terrorist motivation to use this type of attack:

- Sophisticated CBRN agents are potentially highly lethal while being silent killers, and therefore harder to detect and contain;
- Any attack using CBRN material would attract attention and receive prime-time coverage in the mass media;
- CBRN attacks would most certainly provoke terror and panic among civilians;
- CBRN materials have the potential to inflict serious consequences and collateral economic damage;
- CBRN materials offer the means to blackmail governments or at least pressure them;
- Possession and use of CBRN means would place the perpetrator in a position of perceived power vis-à-vis national authorities (at least temporarily) (Dinu 2019, 9).

Other authors also emphasize the fact that for terrorists, one of the major attractions of CBRN weapons is their psychological impact on targeted societies. They also recognize the strategic, operational, tactical, political, and theological motivations for terrorists to use CBRN weapons. Ackerman summarized the following motivation factors: mass causalities, inordinate psychological impact, prestige, incentives for innovation and escalation, mass destruction and area denial, ideology, atomic fetishism, revenge and other "expressive" motives (Ackerman 2005, 2-4).

Also, some authors have an opposing approach, that it is a mistake that this weapon is a desirable choice, and they cite arguments that prove exactly the opposite. The main reason for avoidance of usage is depicted in the negative impact which emerges from difficulty to justify the attack in a moral way, which discourages their sponsors. So, despite numerous advantages that motivate

terrorists to use CBRN agents, certain inhibiting factors can make even terrorists reluctant to be using CBRN agents. In general, there is a:

- General reluctance to experiment with unfamiliar weapons;
- Lack of familiar precedents;
- Fear that the weapon would harm the producer (i.e., radiation) or user;
- Fear of alienating relevant constituencies and potential supporters on moral grounds;
- Fear of unprecedented governmental crackdown and retaliation targeting them, their constituencies or sponsor states;
- Lack of a perceived need for indiscriminate, high-casualty attacks for furthering goals of the group; and
- Lack of money to buy nuclear material on the black market (Matousek 2005, 83).

In the next phase of the research, we investigate the probability that some actor might execute a CBRN attack, which is mostly determined by the motivation of the perpetrator and their capabilities. In terms of CBRN capabilities, analysis of existing literature foresees significantly fewer hurdles to CBRN acquisition for both state and non-state actors in the future, with increasing availability of knowledge, techniques and dual-use materials as a result of knowledge diffusion and economic globalization (Sweijs and Kooroshy 2010, 7–8). Important factors in assessing capacity for attack are also disposable financial resources and personnel, a specific technical knowledge, equipment and CBRN agents. Only when a non-State actor has been able to find sufficient financial support, assembles a network of dedicated and skilled individuals, and acquires the necessary knowledge, equipment and raw materials, the said individual may attempt to build a CBRN weapon (Meulenbelt, Nieuwenhuizen 2015, 847).

Finally, before executing an attack, perpetrators need to select an adequate target. That includes gathering information via observation and surveillance for emplacement possibilities in order to ensure maximum damage. After the target has been chosen, perpetrators prepare a detailed plan that includes transportation to the detonation spot, emplacement, and finally a triggering/detonation mechanism.

Critical infrastructure is a very suitable target for CBRN attacks because the attack results in two very negative effects. A CBRN attack is already devastating by its characteristics, and when we summarize that critical infrastructure represents facilities without which the state cannot function, we see how destructive this attack is. Managing the consequences of CBRN attacks is difficult enough without adding the urgency of returning the object of the attack to function promptly.

2. DETECTION OF CBRN THREATS

The feasibility of CBRN attacks is directly linked to the high number of potential targets which haven't been prepared to handle a CBRN incident. Countering CBRN threats requires effective multi-stakeholder engagement among public and private actors. That includes integrated framework for action to facilitate implementation of preventing policies, regulations and measures to counter misuse of CBRN agents. Novossiolova and Martellini recognized at least five basic components that are essential for establishment, as following: prevention, preparedness and response to CBRN security risks (Fig. 2).

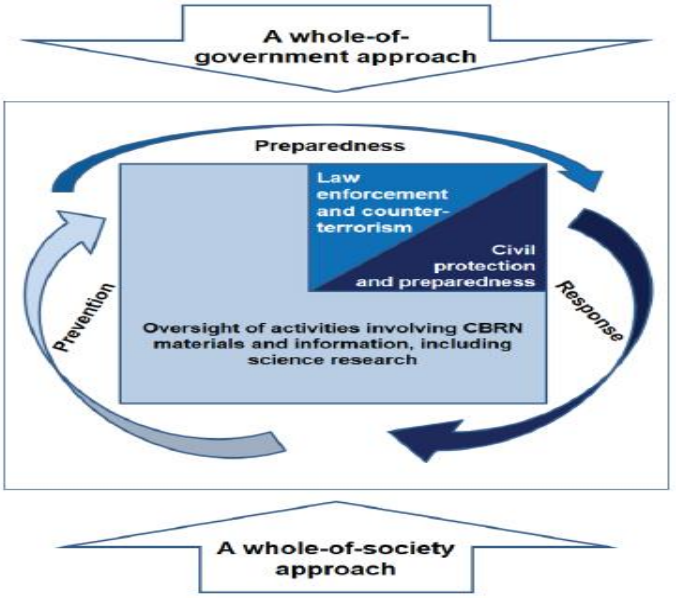


Figure 2 – Key prerequisites for protection from CBRN threats at national level (Novossiolova, Martellin 2021:12).

Three components are thematic and two functional. The thematic elements include: (a) oversight of activities involving CBRN materials and information, including science research; (b) law enforcement and counterterrorism; and (c) civil protection and preparedness. The functional elements include: (a) a whole-of--government approach; and (b) a whole-of-society approach (Novossiolova, Martellin 2021:11). Those key prerequisites for protection from CBRN threats at the national level present the starting point for protection from CBRN threats: oversight of activities involving CBRN materials and information, which is crucial for the prevention of the deliberate misuse of CBRN agents as well as for all following activities.

Namely, as the main precautionary measure is an effort to keep CBRN materials and substances out of reach for any person without authorization to use it. The EU Action Plan defined as its first objective the reduction of accessibility of CBRN materials, meaning better control access to high risk CBRN materials, and optimization of our ability to detect such materials at the earliest stage possible, restricting or controlling access (European Commission 2017, 3). Unfortunately, this is not an easy task to perform, especially because CBRN agents are not rare substances or substances that are not used in various spheres of life. We use term CBRN agent as the generic terminology for CBRN substances in solid, liquid, aerosolized, or gaseous forms that are designed to incapacitate or kill a person. To prevent access to CBRNE agents, security actors must focus on a number of areas, including theft and smuggling; rogue state trade; trafficking; scientist recruitment; orphan sources; the use of toxic industrial chemicals as weapons; dual biotechnologies; dirty bombs; nuclear trafficking; and the nexus of organized crime and terrorist organizations (Galatas 2020, 568). That is the reason why prompted detection of these agents plays a crucial role.

One of the most important factors in preventing CBRN threats is building a security culture of employees that should alert security officer if they notice any

unusual behavior or circumstances. The International Committee of the Red Cross developed an introductory guidance, in which the following potential indicators that will suggest that CBRN attack may occur are identified:

- Suspicious munitions, devices or packages (boxes with wiring, compressed air cylinders with tubing, containers with powders, liquids or aerosols, etc.);
- Oily film or unusual powdery or gel-like substances on exposed surfaces;
- Unusual liquid sprays or vapors in the air, falling on the ground or on exposed surfaces;
- Unauthorized, unexplained or out-of-season overhead spraying in the area;
- Unexplained odors (e.g., smell of bitter almonds, peach kernels, mown hay, cut grass);
- Cases of nausea, difficulty in breathing, convulsions, disorientation, or patterns of illness inconsistent with natural disease reported or confirmed by public health agencies;
- An abrupt spike in the rate of death among animals in the area;
- Low-lying clouds or fog unrelated to weather, clouds of dust or of suspended, possibly colored, particles; and
- People dressed unusually (long-sleeved shirts or overcoats in warm weather) or wearing protective masks (ICRC 2020,11).

Most critical infrastructure facilities have their own security systems that include video surveillance, alarm systems and access control. These security systems have the function of prevention and detection of all threats, so that they can indirectly also detect a CBRN threat. For example, access control can prevent unauthorized entry by a carrier of CBRN agent. However, not only that not all critical infrastructures have this system, but also some characteristics of CBRN agents make them impossible to identify the threat via classical means of protection. For this reason, and in accordance with the characteristics of the critical infrastructure facility, it is necessary to strengthen protective measures by introducing special detectors. The variety of CBRN agents and threats at disposal to possible perpetrators, rise the need for incorporating many detectors into a

single suitable monitoring system and methodology. Thus, depending on a type of critical infrastructure and probability of certain CBRN attack, specific sensors should be chosen as a part of the monitoring and early-warning systems.

In terms of chemical hazards (threats), there are several analytical techniques that could be used for detection of chemical agents or chemical warfare. The main purpose of chemical detectors is to alarm the first responders about chemical threat. Due to this reason, chemical detectors must sign an alarm (signal) as early as possible (i.e., to have fast response). Beside fast response, chemical detectors also need to have as low as possible limit of detection in order to detect chemicals in very low concentrations (ppm or even ppb). Furthermore, selectivity towards specific molecule is necessary to be high.

There are numbers of chemical detectors which can be used in detection of chemical hazards. In the first line, most popular and cheapest detectors are based on ion mobility spectrometry (usually coupled with mass spectrometry (IM-MS)). This technique has been used to separate and identify ionized molecule in the gas phase based on their mobility. There are numerous portable IM-MS devices launched on the market.

Raman spectroscopy and Fourier transformed infrared (FTIR) spectroscopy are very powerful analytical techniques for detection of different unknown substances. Characteristics of both spectroscopies are fast response, low limit of detection and very high selectivity. Raman and FTIR spectroscopies are used for quick detection of different drugs, narcotics, explosives, etc. As in the case of IM-MS detectors, there are numbers of portable Raman and FTIR devices on the market. The main drawback of these instruments is very high price in comparison to the IM-MS.

One of the oldest techniques for detection of chemical warfare is colorimetric detection. This technique is the cheapest in comparison to modern instrumental analytical techniques (IM-MS, Raman and FTIR spectroscopy). This technique is based on color changing of substrate (usually special paper) in touch with chemical agents. It is used only for detection of nerve agents, blister agents and blood agents.

For detection of radiological and nuclear hazards (threats) different detectors for α, β and γ radiations have been used: scintillation detectors, semiconductor detectors, thermal neutron detectors, fast neutron detectors.

Detection of biological threats and hazards (pathogens) are most difficult when compared to the chemical, radiological and nuclear threats. We cannot see, smell or feel biological hazards such as, for example, viruses. Most of them are neither volatile nor dermally active and the first "alarm" for biological terrorism is developed from similar symptoms of the disease in the population (Hülseweh, Marschall 2013). Furthermore, symptoms of disease are often retarded. Usually, detection of biological hazards is based on sampling of different biological samples (such as blood, saliva, etc.) and performed with the use of a technique called polymerase chain reaction (PCR).

3. INTEGRAL RESPONSE TO CBRN THREATS

Countering CBRN threats involves a number of challenges that are similar to those that emerge from the case of conventional threats, but also bring many additional, particular challenges. Depending on the CBRN agent used in attack, its persistency and the actual levels of exposure and contamination, it is possible certain zones and people in that site may remain inaccessible to first responders due to the need for limiting the spread of agents. Calder and Bland have identified at least eight challenges that occur in the case of CBRN attack. First, the presence of CBRN agents complicates accident management for several reasons, starting with increased risk to the first responders from on-scene hazards, as well as contaminated or contagious casualties. Second, the first responder's capability may be diminished due to personal protective equipment such as chemical-resistant suits or gas-tight suits, which require self-contained breathing apparatus. Third, increased risk or anxiety to the wider population is present. CBRN incidents may release plumes traveling beyond the conventional cordons and response zones. Fourth, increased mortality and morbidity of casualties occur. Fifth, an increased number of psychological casualties happen. Also, sixth, casualty processing is

slowed down. Certain hazards will require casualty decontamination before the casualty is transported from the scene, which will be resource, labor, and time intensive. Finally, the management of contaminated wounds may affect surgical management (Calder and Bland, 2015, 441).

In the literature, we can find different response models regarding CBRN attacks, based on risk management, with the main purpose to prepare stakeholders for potential problems that can occur unexpectedly and facilitate anticipating problems in advance. Phases of risk management arise from two basic activities – risk assessment and risk evaluation (Tasić, Ćurčić 2021, 385). These models are very important because they represent the basis for the development of action procedures for a large number of actors. As one of the most complete response models precisely for CBRN attacks, stands out the graphic model that was developed by a group of authors led by Matthew Healy (Figure 3).

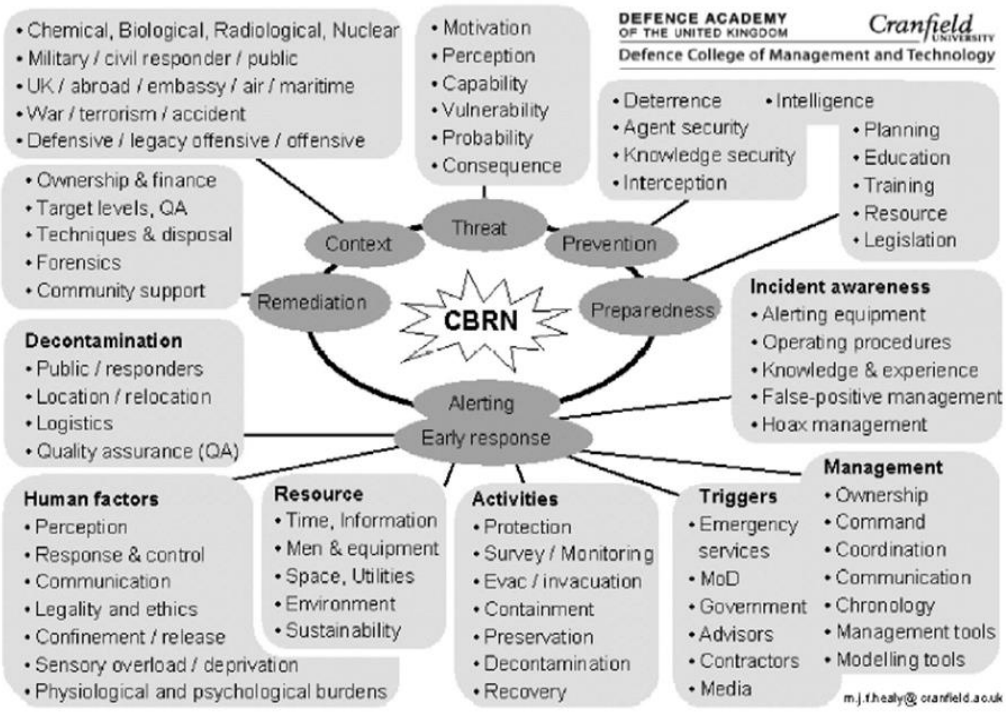


Figure 3 – A Model to Support CBRN Defense
(Healy, Weston, Romilly & Arbuthnot, 2009)

The model was designed to treat the CBRN issue and offer a checklist of underpinning factors which help the planning, equipment development and response processes. The authors explain that, although the chronology of CBRN events is unpredictable and the crisis and recovery phases overlap in practice, the model attempts to build clockwise, starting at Threat (or alternatively Context). The primary groupings are headed as Context, Threat, Prevention, Preparedness, Early Response, and Remediation. The heading 'Early Response' is of such an importance, given that contains such activity and is so diverse and subdivided into Incident awareness, Management, Triggers, Activities, Resource, Human factors and Decontamination (Healy, et al. 2009). This approach advocates a comprehensive approach to organizing timely, coordinated and adequate measures for multidisciplinary, multi-stakeholder CBRN respond. Identification of a different and concrete action in every group of activity represents the main advantage of this model. This model needs to be adapted to the specific object of critical infrastructure and then establish procedures according to specific checklist in every group of activity.

In terms of response to CBRN threat on a critical infrastructure, a major challenge is to build a suitable resilience defined in accordance with the main characteristic of this threat: high consequence low probability events. That factor influences relocation of financial resources to more probable events, mostly with lower consequences. Given that CBRN attack has the most hazardous consequences on unprotected personnel, the main focus should be on appropriate training, integrated into regular activities. Also, the second challenge in providing adequate response is the fact that, in case of CBRN attack, it will not be immediately clear which type of a threat is it from the four possible scenarios (C, B, R, N), nor which agent is involved. Only fully equipped and trained personnel can promptly fulfill that task. Different types of detectors give them the possibility to determine a type of threat and, in some cases, even precisely perform identification of the agent. It is their responsibility to determine the boundaries of the contaminated area, the so

called 'Hot Zone', and to coordinate activities with other public forces (police, medical team, firefighters, etc.). That is why the first responders have a critical role in an overall attempt to keep the consequences at as lower level as possible. In formulating an adequate response, we need to cross all these factors with the basic characteristics of critical infrastructure, which is the fact that the re-functioning of the attacked object must be enabled in the shortest possible time. It implies rapid detection of the used agent in order to promptly undertake activities in the decontamination process as soon as possible after the attack.

CONCLUSION

The potential future use of CBRN agents as weapons depends as much on technology − as it does on geopolitical developments. There will be an increased possibility that CBRN agents might be utilized and deployed as weapons in novel ways, both on the battlefield and in the civil domain, in times of war as well as in times of peace. Although the probability of CBRN attacks is low, the potential consequence is extremely high. Any attack on critical infrastructure is dangerous and with potentially large consequences, and when this threat is combined with the destructiveness of CBRN agents, consequences can be ruinous. Unlike other facilities that may be closed or isolated after a CBRN attack, critical infrastructure facilities must be decontaminated as soon as possible after the attack.

The diversity of characteristics of CBRN agents (toxicity, latency, persistency, and transmissibility) implies a necessity for the usage of different types of detectors, as well as numerous response procedures. This means that the first responders have to apply different detection procedures promptly because the re-functioning of the attacked object must be enabled in the shortest time possible. Those are the main reasons why countries need to invest in protective measures against the CBRN threats, in combination with existing measures of the critical infrastructure object.

REFERENCES

1. Ackerman, Gary, 2006. "Motivations for Engaging in Nuclear Terrorism". In: *Threat Convergence: New pathways to proliferation?* Conference report winter 2006. Washington: The Fund for Peace.
2. Calder Antony, Bland Steven 2015. Chemical, biological, radiological and nuclear considerations in a major incident. *Surgery* (Oxford, Oxfordshire), 33(9), 442–448.
3. Dinu, Elena 2019. "Reassessing CBRN Terrorism Threats". In *Reassessing CBRN Threats in a Changing Global Environment*, edited by Fei Su and Ian Anthony, 8-13. Solna: Stockholm International Peace Research Institute.
4. Galatas Ioannis 2020. Prevention of CBRN Materials and Substances Getting into the Hands of Terrorists. In: *Handbook of Terrorism Prevention and Preparedness,* edited by Alex P. Schmid, 555–587. The Hague, NL: ICCT Press.
5. European Commission 2017. *Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks*. Brussels.
6. Healy, Matthew, Weston, K., Romilly, M., Arbuthnot, K. 2009. "A model to support CBRN defence". *Defense & Security Analysis*, 25(2): 119–135. https://doi.org.
7. Hülseweh Birgit, Marschall, Hans-Jurgen. 2013. "Detection and Analysis of Biological Agents". In: CBRN Protection: Managing the Threat of Chemical, Biological, Radioactive and Nuclear Weapons, edited by Richardt Andre, Hülseweh Birgit, Niemeyer, Bernd, 211–241. New Jersey: Wiley. doi: 10.1002/9783527650163.
8. International Committee of the Red Cross ICRC (2020). *Chemical, Biological, Radiological and Nuclear Response – Introductory guidance,* E-book. Available at: https://shop.icrc.org. (Accessed: 29 September 2021).

9. Matousek Jiri, 2005. "Chemical, Biological, Radiological and Nuclear Terrorism: New Challenge for Protection and Crisis Management". In *Radiation Inactivation of Bioterrorism Agents*, edited by L. G. Gazso and C. C. Ponta, 81-88. Amsterdam: IOS Press.

10. Meulenbelt Stephanie, Nieuwenhuizen Maarten, 2015, "Non-State actors' pursuit of CBRN weapons: From motivation to potential humanitarian consequences". *International Review of the Red Cross*, 97 (899): 831–858. https://doi:10.1017.

11. Mićović Marija 2020. Specifičnosti kritične infrastructure u Republici Srbiji. Beograd: Kriminalističko-policijski univerzitet.

12. Moteff, John, Parfomak, Paul 2004. *Critical Infrastructure and Key Assets: Definition and Identification*. CRS Report for Congress, Congressional Research Service, Library of Congress.

13. Novossiolova, Tatyana, Martellin, Maurizio 2021. *Effective and Comprehensive CBRN Security Risk Management in the 21st Century*. Non-Proliferation and Disarmament Papers. No. 75. Stockholm International Peace research Institute. Available at: https://www.sipri.org. (Accessed: 03 September 2021).

14. Rimpler-Schmid Alexandra, Trapp Ralf, 2021. *EU preparedness and responses to Chemical, Biological, Radiological and Nuclear (CBRN) threats*. Directorate-general for external policies – Policy Department.

15. Sweijs Tim and Kooroshy Jaakko 2010. *The Future of CBRN*. The Hague Centre for Strategic Studies, Vol. 12, No. 3.

16. Tasić Gvozden, Ćurčić Milica, Lazović Ivan 2021. The role of CBRN live agent training in education of first responders. In: *IX International scientific conference "Archibald Reiss Days"*.Thematic conference proceedings of international significance. Edited by Kesić, T. Belgrade: University of Criminal Investigation and Police Studies. p. 379-390. ISBN 978-86-7020-470-6, ISBN 978-86-7020-190-3.

Krešimir Kristić *)

UDC: 351.78:[005.334:004
621.311:[005.334:004

CRITICAL INFRASTRUCURE PROTECTION IN CYBERSPACE

Abstract: *Military strategies define five domains of dynamic operations: land, sea, air, space, and cyberspace. Even in peaceful times, cyberspace abounds with malicious dynamic activities, explosively intensified in periods of conflict. Critical infrastructure is the most effective goal, especially energy infrastructure. The aim of the work is to address the basic guidelines for protecting and achieving resilience of electrical energy infrastructure against Cyberthreats. In relation to the globally prevailing usual functional-security architecture of automation and control systems (IACS) of industrial processes of critical infrastructure, neither effective nor resistant to recognized and recorded attack methodologies on IACS, the paper presents basics of resilient architecture and the basic guidelines for implementation of further organisational, normative and technical measures.*

Keywords: *critical infrastructure, electricity, cyber threats, resilience, protection.*

INTRODUCTION

When speaking of the five areas of dynamic military operations: land, sea, air, space, and cyberspace, even in peaceful times, cyberspace abounds with continuous malicious dynamic activities. Critical infrastructure, especially electricity infrastructure, is the most effective goal. Globally prevailing usual functional-security architecture of automation and control systems (IACS) of industrial processes of critical infrastructure isn't resistant against the recognized and recorded attack methodologies on IACS. It is necessary to find solutions and provide answers to these threats and challenges towards achievement of resilient critical electricity infrastructure. Recognizing the real state of resistance of the critical electricity infrastructure against the threats from cyberspace represents a solid starting point for achievement of this goal.

*) M. Sc. Krešimir Kristić B.Sc.EE, Hrvatska elektroprivreda d.d., Zagreb, Croatia.

1. SITUATION

As we have previously emphasized, malicious activities in cyberspace are constant and unrelenting, with a large number of attacks almost every second on every system exposed on the Internet, regardless of its size, importance, and security. For illustration, Figure 1 shows the Cyberthreat real-time map, based on which it is possible to determine the number of external different types of cyberattacks on the Republic of Croatia during a typical day.

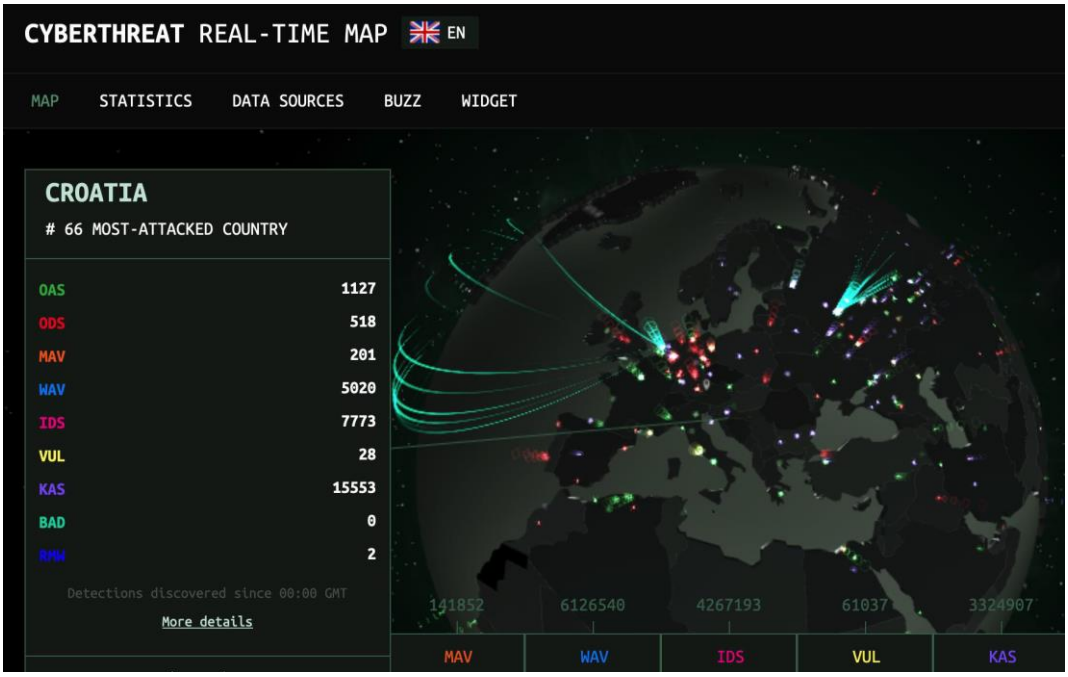


Figure 1 – Cyberthreat real-time map

Furthermore, globally prevailing traditional architecture on automation and control systems (IACS), used in industrial processes of critical infrastructure, as illustrated on Figure 2, when speaking of their design, are resistant to only three of the twenty most sophisticated attack methodologies against operational technologies (OT) of critical infrastructures.

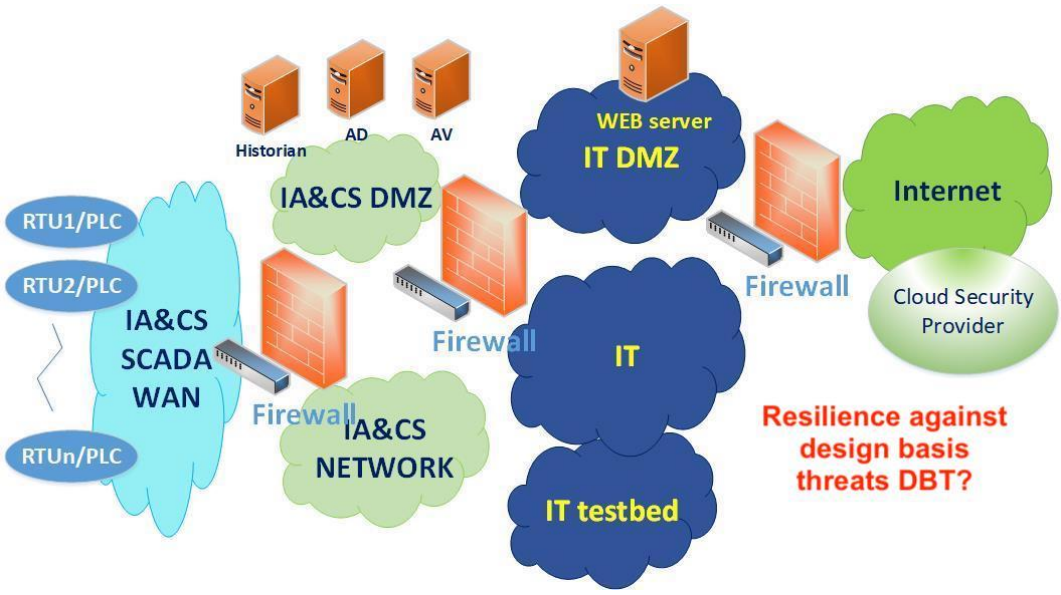


Figure 2 – Traditional globally prevailing functional and security architecture

2. THREATS, RISKS, ATTACKS

Attacker groups are categorized by their motivation, capabilities and sophistication level in the following manner (Kristić 2022, 13):

- Structured organisations
  - State-related Cyber Brigades, Intelligence Agencies – top educated and skilled professionals;
  - Organised crime – Cybercriminal organisations: mafias, gangs, units.
- Ideologically motivated groups
  - Terrorists – Cyber-terrorists, Cyber-militias;
  - Ideological activists – Cyber-hacktivists, interest groups, sects.
- Individual or group of individuals
  - Specialized units and cyber-mercenaries;
  - Amateurs;

- Avengers;
- Pathological attackers – unfair competitors, dishonest clients, scammers, fraudsters.

When examining threats and related risks, as well as the attack techniques and consequences, listed from the first sophisticated attack to the most complex and the most sophisticated, are the following (Ginter 2017, 4-12):

#1 ICS Insider: A disgruntled control-system technician steals passwords by "shoulder surfing".

Risk-Consequences: This class of incident is most often able to cause partial or complete plant shutdowns. More serious physical risk-consequences may be possible, depending on the insider and the details of the industrial process.

Sophistication: This is a moderately sophisticated attack. ICS technicians tend to have good knowledge of how to operate control system components in order to bring about specific goals, such as a shutdown, but less knowledge of fundamental engineering concepts or safety systems designed into industrial processes.

#2 IT Insider: A disgruntled IT insider shoulder-surfs remote access credentials entered by an ICS support technician visiting a remote office.

Risk-Consequences: This class of incident might cause a shut-down, or might just cause confusion. At best, each such incident triggers an engineering review of settings at the plant, to ensure that no physical equipment has been left mis-configured and thus prone to causing a malfunction in the future.

Sophistication: This is an unsophisticated attack. IT insiders generally have little knowledge of cyber systems, control systems or physical processes, but often do have social engineering opportunities that can yield credentials able to log into control system networks.

#3 Common Ransomware: An engineer searching for technical information from an ICS-connected engineering workstation accidentally downloads ransomware.

Risk-Consequences: Most often, the minimum damage caused by this kind of incident is an unplanned shutdown lasting for as many days as it takes to restore the control system from backup, and restart the industrial process - typically 5-10 days of lost production. In the worst case though, important equipment can be irreparably damaged by an uncontrolled shutdown. In this case, replacements for the damaged equipment need to be purchased and installed, and where replacements are not readily available, replacements for damaged equipment must themselves be manufactured, so they can be installed and activated. Worst-case plant downtime in these cases can be up to 12 months.

Sophistication: Authors of autonomous ransomware can be very sophisticated cyber-wise, producing malware that is able to spread quickly and automatically through a network, and even malware that is able to evade common anti-virus systems and other security measures. Such authors, though, tend to have no understanding of physical industrial processes or industrial control systems.

#4 Targeted Ransomware: An attacker with good computer knowledge targets IT insiders with phishing attacks and malicious attachments, gaining a foothold on the IT network with Remote Access Tool (RAT) malware.

Risk-Consequences: Computer, network and other equipment with erased firmware generally must be replaced – the equipment has been "bricked" in the parlance of cyberattacks. Again, an emergency shutdown may damage physical equipment.

Sophistication: The attacker is cyber-sophisticated. Moreover, it is worth noting that we have recorded an increasing trend of organized crime organizations becoming involved with ransomware. These organizations have access to professional-grade malware toolkits and developers, and professional-grade RAT operators.

#5 Zero-Day Ransomware: An intelligence agency mistakenly leaves a list of zero-day vulnerabilities in operating systems, applications, and firewall sandboxes on an Internet-based command and control center.

Risk-Consequences: Again, the minimum damage caused by this kind of an incident is an unplanned shutdown, lasting for as many days as it takes to restore the control system from backups, and restart the industrial process - typically 5-10 days of lost production. In the worst case though, important equipment can be irreparably damaged, necessitating costly replacement, which may take additional weeks or months. Sophistication: Cyberattacks only become more sophisticated over time. Security researchers and others discover zero-day vulnerabilities, and intelligence agencies have been known to "lose track" of the zero-days they have discovered or purchased. This attack is usually very sophisticated cyber-wise, but unsophisticated engineering-wise.

#6 Ukrainian Attack: A large group of hacktivist-class attackers steal IT remote access passwords through phishing attacks.

Risk-Consequences: In the case of the attacks conducted in Ukraine, power was shut off to over 200,000 people for up to 8 hours. Power was only restored when technicians travelled to each of the affected substations, disconnected control system computers, and manually turned the power flows on again. More generally, unplanned shutdowns are a consequence of this class of attacks, and possibly emergency, uncontrolled shutdowns with potential equipment damage that accompanies such shutdowns. Sophistication: This is a summary of the attack techniques used in the 2016 attack on a number of Ukraine electric distribution companies. The attackers had good knowledge of cyber systems, but limited knowledge of electric distribution processes and control systems.

#7 Sophisticated Ukrainian Attack: A more sophisticated group of attackers use the techniques of the Ukraine attack, but are more sophisticated when speaking of the use of cyber-attack tools and engineering details of electric systems.

Risk-Consequences: Risk-Consequences of this attack are more serious. For example, at one such occasion, many large refrigerators in grocery stores have been rendered inoperable, large water pumps in water distribution systems are similarly damaged, and a large number of smaller pieces of equipment in

consumers' homes were rendered inoperable. High voltage transformers must be replaced on an emergency basis, which takes over a week. There is no world-wide inventory of such transformers, so while replacement transformers are manufactured, emergency replacements are acquired by reducing redundancy and capacity in other parts of the electric grid.

Sophistication: This group of attackers is moderately sophisticated, both cyber-wise and engineering-wise.

#8 Market Manipulation: An organized crime syndicate targets known vulnerabilities in Internet-exposed services and gains control over IT networks.

Risk-Consequences: Lost plant production and emergency equipment repair costs.

Sophistication: Cyber-sophistication of this attack and these attackers is moderate – no zero-days are used, and no code is written. Engineering sophistication of this attack is high. The attackers need access to an engineer able to interpret the control system configurations, select physical equipment to target, identify the PLC controlling that equipment, download the existing program of that PLC, and design and upload a new program able to wear out the targeted physical equipment prematurely, while reporting to the HMI that the equipment is operating normally.

#9 Sophisticated Market Manipulation: More cyber-sophisticated attackers carry out the market manipulation attack, but in a way that is harder to defend against. They use known vulnerabilities in Internet-facing systems to compromise the IT network of a services company known to supply services to their real target.

Risk-Consequences: Lost plant production and emergency equipment repair costs.

Sophistication: Cyber-sophistication of this attack and these attackers is high. No zero-days were used, but the attackers developed custom malware with steganographically-encoded communications. The engineering sophistication, like the Market Manipulation attack, is high.

#10 Cell-phone WIFI: Sophisticated attackers seek to inflict damage on a geography they are unhappy with for some reason. The attackers create an attractive cell phone app – call it the world's fanciest free flashlight app. The attackers use targeted social media attacks to persuade office workers at critical infrastructure sites in the offending geography to download the app, which requests more permissions than a flashlight app should request, but these workers are not cyber-sophisticated and think nothing of it.

Risk-Consequences: Repeated plant shutdowns from a source that is difficult to identify. Plant personnel should eventually determine that the source of the attack is a WIFI network and shut down all WIFI at the plant, or at least change all the passwords. Sophistication: This attack at this moment needs a high degree of cyber-sophistication, because toolkits enabling this kind of hidden WIFI hacking from cell phones currently do not exist on the open Internet, and thus the attackers need to write this malware themselves, or buy it. Once such attack tools are widely and publicly available, this class of attack will come within the means of hacktivist groups annoyed with industrial enterprises. The attack needs only very low engineering sophistication.

#11 Hijacked Two-Factor: Sophisticated attackers seek to compromise operations at an industrial site protected by best-practice industrial security.

Consequence: Any attacker willing to invest sophisticated, custom malware in this kind of attack is most likely going to persist in the attack until significant adverse outcomes are achieved.

Sophistication: Currently this requires a high level of cyber-sophistication, since no such two-factor-defeating remote access toolkit is available for free download on the open Internet. In order to inflict a serious physical consequence within a limited number of remote access sessions, a high degree of engineering sophistication as well should be implemented as well.

#12 IIoT Pivot: Hacktivists annoyed with the environmental practices of an industrial site learn from the popular press that the site is starting to use new, state-of-the-art, Industrial Internet of Things edge devices from a particular vendor.

Risk-Consequences: Unplanned shutdowns, lost production, and possible equipment damage.

Sophistication: These attackers are of moderate cyber-sophistication. They can download and use public attack tools that can exploit known vulnerabilities, they can launch social engineering and phishing attacks, and they can exploit permissions with stolen credentials. Hacktivists usually have a very limited degree of engineering sophistication.

#13 Malicious Outsourcing: An industrial site has outsourced a remote support function to a control system component vendor – for example: maintenance of the plant historians. The vendor has located their world-wide remote support center in a country with an adequate supply of adequately-educated personnel, low labor and other operational costs. A poorly-paid technician at this support center finds a higher-paying job elsewhere, and before leaving, decides to take revenge on personnel at a particular industrial site - personnel who complained to the technician's manager about the technician's performance.

Risk-Consequences: Risk-Consequences of such an attack vary. For example, no power plant relies on the veracity of its historians for second-by-second operation – at such a target, if the historians were targeted, the risk-consequences would be the loss of historical data since the last backup. Historians targeted at a pharmaceutical plant would likely trigger the loss of the current batch, since many such plants store their batch records in the historians, and are unable to sell product for batches whose records are impaired. Such batches can range in value from hundreds of thousands of dollars to hundreds of millions of dollars.

Sophistication: This is an adversary with limited cyber sophistication or engineering sophistication, who is unable to produce custom malware. This attacker does have credentials and the ability to log into their target remotely, and has some knowledge of how that system works – in particular, how to leave a small, simple script running, or schedule such a script to run in the future with administrative privileges.

#14 Compromised Vendor Website: Most of us trust our ICS vendors - but should we trust their websites? Hacktivists find a poorly-defended ICS vendor websites and compromise it.

Risk-Consequences: Most often, the risk-consequences of this class of attack are depicted in an unplanned shutdown. However, if enough of the control system is affected by a simultaneous shutdown, failure may trigger an uncontrolled shutdown which, in many industries, risks equipment damage.

Sophistication: This is a hacktivist-class attack, usually conducted by attackers of moderate cyber sophistication and limited engineering sophistication. The attackers know enough about computer systems to use existing tools, permissions and vulnerabilities. They have enough knowledge to unpack control system products and understand to some degree how they work, as well as unpack and re-pack security updates.

#15 Compromised Remote Site: SCADA systems are control systems that use wide-area-network communications, such as power grids and pipelines. In such systems, remote sites, such as substations and pumping stations, are typically unstaffed, with limited physical security, such as a wire fence, locks and perhaps video surveillance. In this scenario, an attacker physically cuts the padlock on a wire fence around a remote station and enters the physical site. The attacker locates the control equipment shed - typically the only roofed building at the site - and again, forces the door to gain entry to the shed. He walks over to the only rack in the site, plugs a laptop into the switch, and tapes it to the bottom of a piece of computer equipment low in the rack where it is unlikely to be detected. The attacker leaves the site.

Risk-Consequences: Interruptions of movement of electricity, natural gas, water, or whatever else the remote station manages represent the simplest consequence of this class of attack. Erased hard drives are another simple consequence. Attackers with a higher degree of engineering sophistication could reprogram protective relays or other equipment protection gear, damaging physical

equipment such as transformers and pumps. More sophisticated manipulation of pipeline equipment, especially in liquid pipelines, can result in pressure waves able to cause pipeline breaches and leaks. Sophistication: This attack requires physical access to at least one of the remote sites, and an investment of physical risk, as well as equipment - the laptop. Hacktivist-class cyber expertise is needed to break into the remote site and the central site. Very limited engineering expertise is needed to bring about a Ukraine-style consequence.

#16 Vendor Back Door: A software developer at a software vendor inserts a back door into software used on industrial control systems networks. This may be ICS software, or it may be a driver, management, operating system, networking, or other software used on the ICS network. The back door may have been installed with the blessing of the software vendor, as a "support mechanism," or may have been installed surreptitiously by a software developer with malicious intent.

Risk-Consequences: Plant shutdowns and erased hard drives are easily inflicted by hacktivist-class attackers who have carried out this kind of attack before. More engineering-sophisticated attackers can most likely cause equipment damage, and sometimes even put worker safety or public safety at risk.

#17 Stuxnet: Sophisticated attackers target a specific and heavily-defended industrial site. They first compromise a somewhat less-well-defended services supplier, exfiltrating details of how the heavily-protected site is designed and protected. The adversaries develop custom, autonomous malware to target that one site and cause physical damage to equipment at the site. The autonomous malware exploits zero-day vulnerabilities. Service providers carry the malware to the site on removable media. Anti-virus scanners are blind to the custom, zero-day-exploiting malware.

Risk-Consequences: For example, the Natanz uranium enrichment site targeted by Stuxnet is thought to have suffered several months of reduced or zero production of enriched uranium, because of the interference of the Stuxnet worm

in the production process. The site is also estimated to have suffered the premature aging and destruction of 1,000-2,000 uranium gas centrifuge units. More generally, this class of attack can bypass all but physical safety and protection equipment, and could cause loss of life, public safety risks and costly equipment damage.

Sophistication: This class of attack demands high degree of engineering sophistication, as well as understanding the the physical process and control system components, and bypass equipment protection and safety systems with an attack. The attack demands a high degree of cyber sophistication as well in order to encode that new attack into custom malware that is undetectable by the specific cyber security technologies deployed at the target site.

#18 Hardware Supply Chain: A sophisticated attacker compromises the IT network of an enterprise with a heavily-defended industrial site. The attacker steals information about which vendors supply the industrial site with servers and workstations, as well as which vendors routinely ship that equipment to the site. The attacker then develops a relationship with the delivery drivers in the logistics organization, routinely paying the driver modest sums of money to take 2-hour lunch breaks, instead of 1-hour breaks. When IT intelligence indicates that a new shipment of computers is on its way to the industrial site, the agency uses the 2-hour window to break into the delivery van, open the packages destined to the industrial site, insert wirelessly-accessible single-board computers into the new equipment, and then re-package the new equipment so that the tampering is undetectable. Some time after the IT records show that the equipment is in production, the attackers access their embedded computers wirelessly in order to manipulate the physical process. The attackers eventually impair the equipment protection measures, crippling production at the plant through what usually appears to be a long string of very unfortunate, random, equipment failures.

Risk-Consequences: Costly equipment failures and plant production far below targets.

Sophistication: This is an attack conducted by a very sophisticated adversary. This attacker has the physical "man in the field" dor carrying out covert actions, such as breaking into the delivery van and quickly disassembling, modifying, re-assembling, and re-packaging the compromised equipment. The attacker is cyber-sophisticated, maintaining a long-term presence on the target's IT network, and understanding the design of a variety of computer equipment enough to understand how to subtly insert additional hardware into that equipment. The attacker has a high degree of engineering sophistication as well, necessary to understand the structure of the physical process, control systems, and equipment protection systems enough to design and carry out physical sabotage and make the damaged equipment look like random failures.

#19 Nation-State Crypto Compromise: A nation-state grade attacker compromises the PKI encryption system, either by stealing certificates from a well-known certificate authority, or by breaking a popular crypto-system and forging the certificate. The attacker compromises Internet infrastructure to intercept connections from the site to software vendors, and deceives the site into downloading malware with what appears to be legitimate vendor signatures. The malware sets up peer-to-peer communications, steganographically tunnelled through ICS firewalls and DMZs on what appears to be a legitimate vendor--sanctioned communications channel. The nation-state adversary operates the malware by remote control, learning about the targeted site. The adversary creates custom attack tools which, when activated, cause the release of toxins into the environment, serious equipment damage and a plant shutdown.

Risk-Consequences: Public safety risks and possible loss of life, costly equipment damage and lost production.

Sophistication: This is a very sophisticated adversary able to defeat the encryption, certificates, signing and cryptographic hashes that are the foundation of many security programs.

#20 Sophisticated Credentialed ICS Insider: A sophisticated attacker bribes an ICS insider at an industrial site. The insider systematically leaks information to

the attackers about the design of the physical process and the industrial control system. The attacker develops custom, autonomous malware. The insider deliberately releases the malware on the system with the insider's credentials. A few hours later the malware activates. A day later, there is an explosion that kills a number of workers, causes a billion dollars in damage to the plant, and shuts the site down for 12-18 months.

Risk-Consequences: Loss of life, costly equipment damage and lost production.

Sophistication: This is an attacker with a high degree of sophistication in physical operations, given that such operations demand bribing the insider, but also a high degree of engineering sophistication, necessary to determine what cyberattack has not been anticipated by the site's safety and equipment protection systems, or to determine how to defeat those protections, and a high degree of cyber sophistication to produce undetectable, custom, autonomous malware.

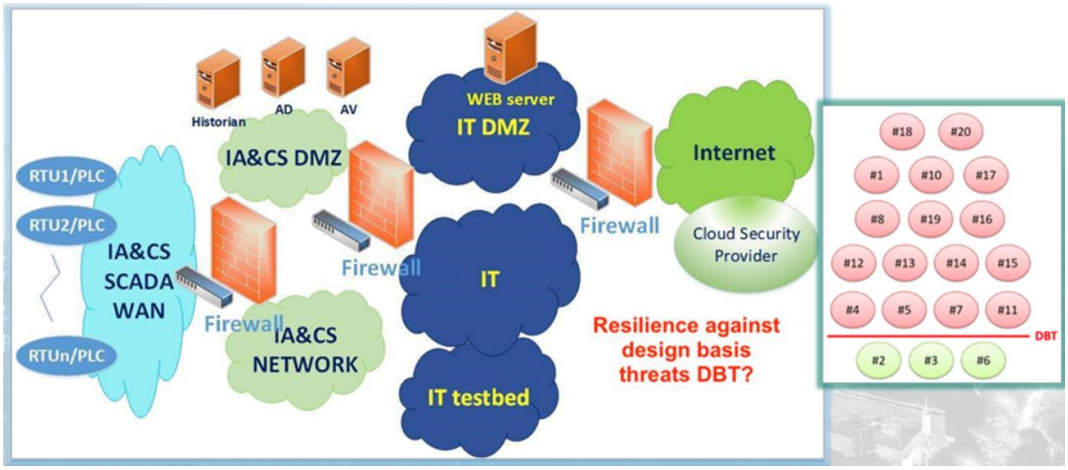


Figure 3 – Traditional IACS poor resilience against design basic threats

Traditionally postured IACS of critical infrastructure by their design are resistant only on three of the twenty mentioned most sophisticated attack methodologies against the operational technologies (OT) of critical infrastructures.

3. RESILIENCE OF ELECTRICITY INFRASTRUCTURE

The improved security-functional architecture of IACS, based on Unidirectional Gateways and best implemented as Data Diodes, significantly increases resilience. However, the transition of traditionally postured IACS of critical infrastructure is not that easy, nor can it be done quickly. The primary requirement for electrical energy critical infrastructure is to ensure the continuity of functioning, that is, the reliability and availability of core industrial processes, plants and facilities. It is generally known that the change in management of industrial production plants and facilities is an extremely demanding, complex and, as a rule, lengthy process. Transition towards the improved IACS functional and security architecture, based on Data Diodes, is quite a demanding project.

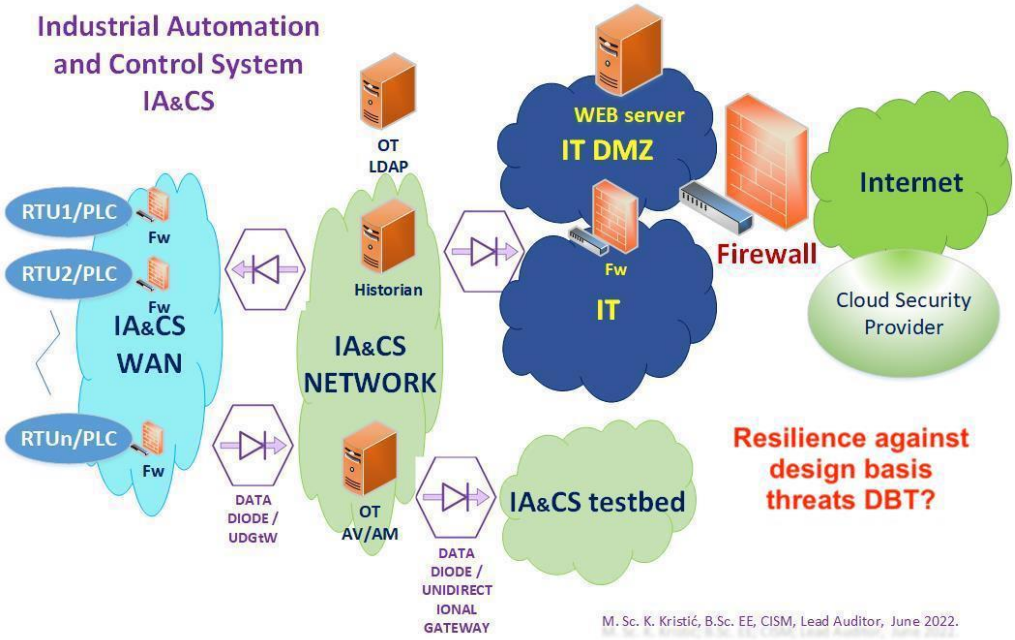


Figure 4 – Improved IACS functional and security architecture

CONCLUSION

At the very least, it is necessary to implement functional and security-wise traditional architecture as a minimum. Further, in the organizational and normative field of cyber security of critical infrastructure, two crucial steps are necessary.

Applcation of the following relevant sectoral regulation at the pan-European level of the EU and the related laws of the member states, as well as the best practices primarily defined in the families of standards:

- ISA/IEC 62443 – security of industrial automation and control systems,
- ISO/IEC 27000 – information security management system,
- ISO/IEC 22300 – business continuity management system and
- ISO/IEC 28000 – supply chain security management system,

and subsequently in other applicable standards, should enable definition and implementation of holistic comprehensive cyber security programs for industrial automation and control systems (Program).

On the organisational and technical level, the Security Operations Center (SOC) is a must. It acts as the first line of defence against cyber threats and provides round-the-clock 365-days-yearly monitoring for cyber threats and the ability to engage immediately in incident response.

Figure 5 – SOC: 24 × 7 × 365 real-time risk detection and incident response

With these achievements, it is possible to carry out a transition towards a significantly improved IACS security architecture, based on Data Diodes, and raise resilience.

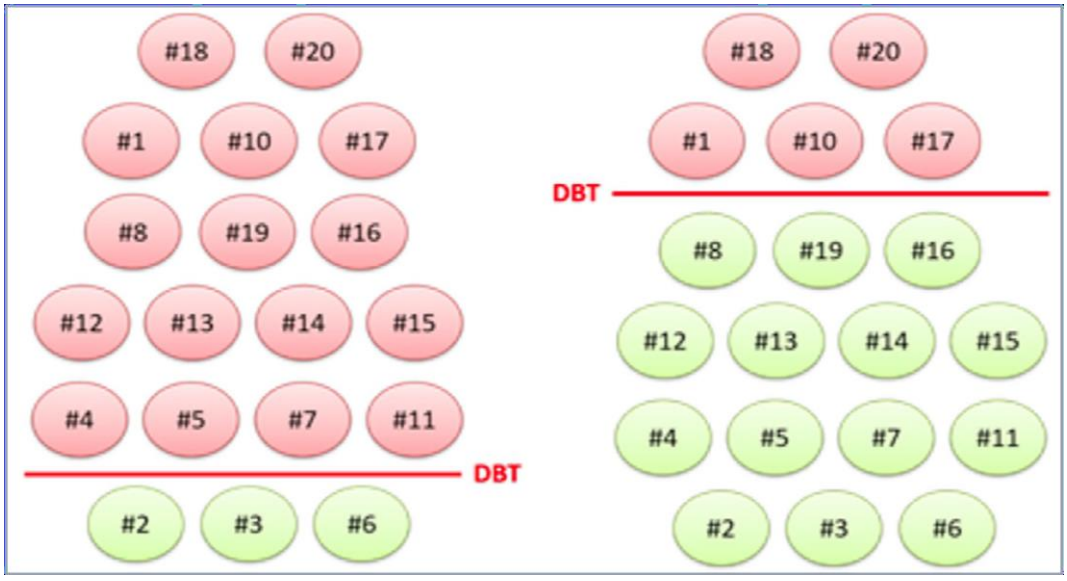


Figure 6 – Resilience of traditional and improved security architecture against the threats (Ginter 2017, 18)

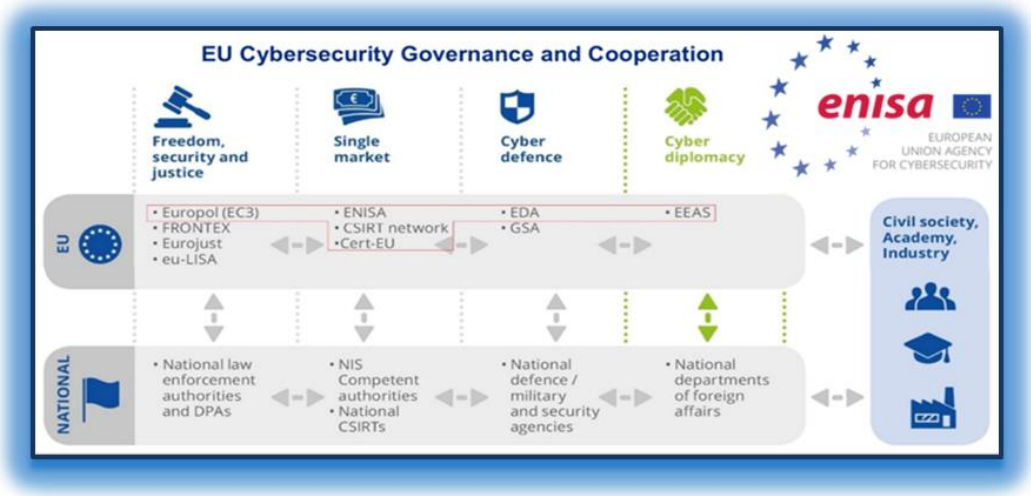


Figure 7 – EU Cybersecurity Governance and Cooperation (ENISA 2017, 17)

Implementation of the Program, which includes transition to an improved security architecture with a functional SOC at the operational level, as well as cooperation and coordination with competent authorities and institutions at the national and EU level, provides resilience above the usually reached level.

REFERENCES

1. Ginter, Andrew, ed. 2017. *The Top 20 Cyberattacks on Industrial Control Systems* Ashburn, VA, USA: Waterfall Security Solutions Ltd.
2. Kristić, Krešimir, ed. 2022. *Kibernetička sigurnost distibucijskih elektroenergetskih sustava*. Zagreb, Croatia: University of Zagreb, Faculty of Electrical Engineering and Computing.
3. ENISA, ed. 2017: *Principles and opportunities for a renewed EU cybersecurity strategy Version B* Heraklion, Greece.

Sergey Cvetkovski*)
Goran Zendelovski**)
Vančo Kenkov***)

UDC: 351.78:[005.334:004
355.58:004

CYBER DEFENSE CAPACITIES OF CRITICAL INFRASTRUCTURE

Abstract: *The paper presents a review of the capacity of civil society to counter attacks on critical infrastructure. Given the prevalence of cybernetics in the near future, the paper suggests that countries will be subject to a number of surprise IT attacks. The paper then provides an overview of the concept of critical infrastructure protection, including the lack of civilian capabilities that could adversely affect defense power of even the great military powers. The development of civil defense against cyber-attacks in the period after the end of the Cold War will be briefly outlined. The authors of the paper will use qualitative analysis of the numerous data on critical infrastructure and cyber-attacks to explore the need for a new paradigm of change in defense policies and appropriate actions. The assumption is that there is currently a low level of such activity globally, especially for extreme emergencies. Questions are asked about cyber defense vulnerabilities and how to counteract recorded vulnerabilities accordingly. The conclusions will point to the challenges of reform, priorities and budgets in joint defense capabilities.*

Keywords: *Cyber Attacks, Critical Infrastructure, Capabilities, Defense, Civil Defense*.

*) Associate Professor. Institute for Security, Defense and Peace at Faculty of Philosophy, Ss Cyril and Methodius University – Skopje.

**) Associate Professor. Institute for Security, Defense and Peace at Faculty of Philosophy, Ss Cyril and Methodius University – Skopje.

***) Professor. Institute for Security, Defense and Peace at Faculty of Philosophy, Ss Cyril and Methodius University – Skopje.

INTRODUCTION

With the start of the "special military operation" of the Russian Federation in Ukraine, a new Cold War era has dawned for the world. Was the military conflict in Ukraine really a surprise for the majority of countries in the world, or maybe such events were expected and planned? Perhaps the specific event was indeed a surprise in a strategic sense for almost all European states, but this type of intervention is not completely unknown and unpredictable on the world scale. The proof for this, or even better proof that the great powers in the past 30 years have not at all abandoned the concept of preparing and living in a Cold War state, is that the governments of the richest countries have individually allocated hundreds of billions of dollars to purchase new weapons systems for the next three decades of design for a major war contingency. Some of those governments have yet to rethink their plans and budgets for the civilian capabilities that will then be needed to protect national cyber resilience, both to support their military operations and to protect their own civilian population. A major war in the near future, as the current state of hostilities in Ukraine indicates, will be dominated by new advanced killing technology and mass information operations. Such a war will increasingly be characterized by highly informational sophisticated autonomous weapon systems, and military robotics, all of which depend on advanced information technologies that will certainly be subject to attack by adversaries.

In that sense, the focus of the states must be placed on the following concept: cybernetic attack/assault. As a result, there will be an investment in the context of cyber civil defense planning. For more than a decade now, the significance of the conflict in cybernetic space has been highlighted, and the probability of such a large conflict is increasing more and more. Pointing out the possibility of a cyber assault at the conflict level is one level away from a cyber-attack, as it has been implied until now. Whether it is at the level of an attack or at the level of an

assault, it is a challenge (for national defenses and a challenge in the scientific sense) that deserves a direct and extensive analysis in the form of determining the civilian capabilities to deal with a national cyber crisis that is taking effect on national security.

Hence, the question arises as to how states (which are military and economic powers) should plan national defense against unexpected cybernetic attacks, including mass information warfare. The purpose of such a cyber-attack would be to prevent the enemy's sophisticated combat systems from being deployed to a position of use, disable them, disrupt the command and control, and prevent civilian sector support (including political support) to the armed forces of the enemy. Here we must also point out the diluted concept of national security and national territory that have undergone transformation with globalization processes and with the particularities of the information space, especially its complicated non-sovereignty of information and communication technology that underpin everyday modern life, both within domestic state borders and beyond (Austin 2019, 1).

Then, there are some questions about the wider concepts of civil preparedness, civil support and civil defense that would be applied in such emergency military situations. This in turn is connected with some newly appeared visible policies that single out only certain large military powers. The impact of an inadequate strategic policy on civilian capacity weaknesses is that highly vulnerable states with low response capabilities will have limited opportunities to shape coercive pressure on their adversaries.

A review of the available literature on cyberspace dependencies indicates a low level of visible engagement outside US research centers on the political dynamics of cyber civil defense in extreme contingencies. The overall analysis of such political dynamics must be guided by several assumptions: comprehensive (absolute) protection of information systems is impossible; in a situation of war

between states, risk management – which, if approached like peacetime business management, based on balancing the benefits against the costs of investments in cyber defense, under conditions of war or imminent war – will be inapplicable; a nation's cyber security is not just the sum total of the cyber security of its enterprises, government agencies and military – it is much more. The sense of security that national cyber security planners may feel from helping enterprises improve their security is insufficient to represent the national cyber civil defense.

A national cyber security strategy should not only be in line with the global state-of-the-art computer security research and development, but it should also anticipate scientific research and technological advances that may in turn either impede or transform its functionality.

1. CYBER-ATTACK AND CYBER ASSAULT

1.1. EXERCISES TO RESPOND TO CYBER ATTACKS

In 2016, the website of the Department of Homeland Security in the United States published a full report on a series of five exercises on the response of civil society to cyber-attacks in the period 2006 - 2016. In 2018, another 6th exercise of this exercise type was conducted. Overall, the goals set by the Department of Homeland Security were the following:

- to examine the ability of organizations to prepare, protect and respond to the effects of cyber-attacks;
- to exercise strategic decision-making and interagency coordination of incident response in accordance with policies and procedures at the national level;
- confirm information sharing links and communication pathways for gathering and disseminating cyber incident situational awareness, response and recovery information; and
- to examine the means and processes through which sensitive information is shared across borders and sectors without compromising proprietary or national security interests.

In the first exercise, held in 2006, the civilian community came together for the first time to examine the national response to cyber incidents. In the second exercise, in 2008, the scenario was cyber-attacks on persistent, imagined adversaries with different political and economic agendas. The abilities of individual response and decision-making among the management was tested. The third exercise, in 2010, provided the first operational test for the NCCIC (National Cyber Security and Communications Integration Center). As the fourth Cyber Assault Exercise, 15 core exercises were conducted between 2011 and 2014 to assist local communities and states in practicing cyber response capabilities in escalating incidents. The fifth exercise, in 2016, involved more than 1,000 distributed players and brought together new sectors, including participants from retail and healthcare. The sixth exercise in 2018 focused on critical production and transportation sectors with the participation of information technology and communications sectors, police, defense and intelligence agencies; state and local administration; and international partners (CISA 2018).

1.2. CYBER STORM CONCEPT

The DHS's concept of a cyber storm appears to fit the official US definition of a "Significant Cyber Incident", when "one (or a group of related cyber incidents that together) is likely to result in visible harm to national security interests, foreign relations, or the economy of the United States or the public trust, civil liberties, or the public health and safety of the American people" (White House 2017).

It is possible to identify three levels of response at the national level to cyber security in a broader sense: 1. Regular common cyber security practices; 2. Advanced persistent threat – the more sophisticated the crime and the more persistent the cyber campaigns against the state, the more strategic partnership between industry and government will be required to respond; 3. Low frequency

but high negative impact events, such as catastrophic and possibly cascading events that are likely to require significant time for assessment, response and recovery (Stacey 2015).

Resilience plans should assume pervasive uncertainty. It means rejecting the traditional trust relationship of everyday routine communications and expecting a malicious actor or actions to be part of a normal functioning. Resilience programs should be designed to mitigate such actions. All of this promotes a paradigm shift in the methods that have been used until now for the development of control systems.

Aside from the experiences of the US Department of Homeland Security exercises, several other governments have also developed the concept of cyber storm. Such an example is Australia. In 2016, Australia's Cyber Security Minister Dan Tehan gave a public speech warning the country to be prepared for a cyber assault. Such a speech represented a reversal of the previous government policy of underestimating cyber threats at the national level in order to avoid the emergence of unnecessary anxiety among the population. The scenario presented by Tehan was simple, yet impactful: The power goes out across most of one of the major cities; street lights and traffic lights go out, mobile and fixed telephony is dead; power surges damage power generators that are powered by the electrical network; coordination efforts stall because each communication structure is burdened with demands; chaos reigns as people panic, leading to damage and loss of life; local businesses must return to cash and ATMs are down; it takes weeks to restore power in some areas, and in the meantime, the local economy is frozen. The reason for this hypothetical situation was an attack against a power company with a cyber virus introduced into its systems through a certain subcontractor with a simple method – a simple opening of an email (Austin 2019, 3-4). This scenario sets up catastrophic cascading effects from a single vector, one-time cyber-attack.

The concept of cyber storm is neither theoretically precise nor legally defined yet. But it is still a concept that in some countries for key stakeholders is a means to organize a response to severe cyber crises at the national level. Although closely related to the contingencies of large-scale warfare in cyber space, the Cyber Storm concept retains great relevance for high-level non-military planning and contingencies in peacetime or wartime. One of the primary benefits of the "cyber storm", at least as a term of art, is that it can be a means of politically mobilizing new forms of civil society capacity (such as civil defense) that are likely to give the most significant role to the non-cyber emergencies' governance agencies in most countries.

1.2.1. SMALL ATTACKS, BIG CONSEQUENCES

The concept deserves additional analysis on two issues: local effects and frequency or numbers. Basically, a Cyber Attack will have local effects even if it occurs as a Cyber Assault that leaves national effects. Cyber assault will often manifest as a series of unrelated attacks on local systems that occur differently in any of the subsystems that affect the cyber resilience/resiliency.

In the theory of general cyber security, there are eight basic elements that make up cyber security, five of which are of a technical nature (hardware, software, payload, networks, power supply) and three that are not of a technical nature (people, politics and ecological systems). In preparing for a cyber assault, it is important to understand the three non-technical elements, because what has been less clear in all cyber-attack exercise scenarios precisely include the influence of local social factors that interact in a unique way with the national (proper) scene: the national people, national politics and national environmental systems.

The suggestion that infrastructure itself can direct cascading consequences is quite significant here (Pescaroli and Kelman 2017). The unique ways in which inherent local features are set up or operate will impose additional complexities in a cyber-attack. The importance of local (or regional) attitudes leads to the emergence of regional bodies or mechanisms to respond to needs.

Second, a cyber assault – where an attack has to be carried from one state to another – would likely be multi-vectored (using hundreds of "tools" in the cyber arsenal); would include polymorphic malware (APTs); would be sustainable; at multiple locations, including civilian and military targets; would affect planned (strategic) goals and accidental unplanned goals; would be accompanied by targeted social influence (information campaigns); and on top of all that, it would have unpredictable and predictable cascading effects. Examples of known or planned attacks are provided so that any responsible state could at least consider them when preparing for a cyber-attack carried out by another state: blackmail when blocking computer access, attack on industrial process control software (such as the Stuxnet 2010 case), disruption of functioning of satellites, dissemination of confidential data from key people in the security sectors, cutting underwater communication cables, blocking civilian satellite links, preventing the transmission of electricity by direct physical damage to power lines (such as when NATO used graphite bombs in Yugoslavia in 1999), spreading false data in military systems, attacking banks, attacking oil companies with modulated computer viruses, attacking the software of civil airline companies, attacking nuclear power plants and hydropower plants, disrupting all civilian communications, etc. In preparing for a cyber assault, the approach should be a harsh extreme scenario of complex, multi-faceted attacks on a continuous basis over prolonged periods.

1.2.2. TIME FOR THE CYBER ASSAULT

The question arises about the future of cyber warfare. At the level of the general trends of political debate and planning of defense against cyber weapons, there is very little consideration of the political use of cyber weapons that is transformed when it is among the arsenals of such weapons and where states create doctrines to combat multi-vector warfare, multi-wave, preventive and sustained cyber campaigns such as the ones previously mentioned. What will cybernetic arsenals look like in the next two to three decades? What will the technical methods of cybernetic assaults look like in that time frame? Will the states plan to use their cybernetic arsenals? Currently, the concept of cyber assault is not only not widespread, but has not been formally adopted by any state in its military or strategic planning. However, the reverse is very likely and even inevitable.

The concept of cyber assault is related to lightning warfare (*blietzkrieg*), which involves having a weapon that only you have and that can be deployed/used at lightning speed. This has important connotations for strategic choices between defensive and offensive strategies, including the all-important concept of pre-emptive strike (Austin and Sharikov 2016). At the core of the offensive propensity in cyber operations is the idea of forcing the outcome of a war quickly and suddenly at the outset by ruthlessly engaging cyber assets rather than a country's "total combat power".

It is a matter of time before states plan to be able to conduct offensive cyber operations at all levels of command in time of war. Such a plan includes attacks on civilian infrastructure associated with the war effort, including - in case of military necessity – possibly against civilian nuclear power plants and dams. This means that such states have accumulated arsenals of various cyber weapons to enable a multi-vector, multi-wave, preemptive and sustained attack on an adversary's military and civilian infrastructure.

2. CIVIL SUPPORT, CIVIL PLANNING: CONTESTED POSSIBILITIES

By the end of the cold war, there was a widely used notion of civil defense. It is not just a term, it was a system (subsystem of the defense system) with its own recognizable subsystem of civil protection (protection and rescue), with its own tasks and activities (sometimes even) of strategic importance. It was simultaneously a policy of the state to deter a potential adversary with nuclear weapons, but also simply a policy of the state for humanitarian insurance, crisis control and survival of the state from hostilities and accidents both in war and in peace.

The use of the civil defense notion has been significantly reduced since the beginning of the nineties of the previous century, given that, in parallel, the civil defense systems were terminologically changed with introduction of more colorful terms, such as crisis management, that is, management of emergency situations. However, despite the reduced social visibility of the civil defense system and its strictly defined organization in the legal sense, the essence of the civil defense system remains the same, i.e., it is unchanged in today's successor systems (such as crisis management, civil protection, protection and rescue, etc.) and it is as the following: a set of measures that, in crisis and defense situations, ensure the existence, efficiency of military defense and the life of citizens in the country. In the old-new forms in which it appears as civil support and civil planning, the former system of civil defense continues to be a system that ensures the survival of the population, functioning of the political system, as well as supports the military defense, making human and material potentials, without which military defense cannot be accomplished, available to it. That system continues to be "a set of preventive and rescue preparations that are carried out, organized or similar, for the purpose of protecting the population and economic facilities from modern types of means of attack and destruction, as well as for the purpose of removing the consequences of catastrophes, natural disasters and malfunctions" (Sukjenik 1976, 5).

The concept, idea and policies of civil defense have been quite controversial in the past. In a book written on civil defense policies in response to the threat of nuclear war, Vale (1991, 13) describes the idea of civil defense as unpopular and disturbing. While in peacetime the burden of thinking about the subject may be assigned to political leaders (such as bureaucrats and academics), the burdens of implementing civil defense measures both in the times peace and war "are physical and directly affect everyone's citizen daily life". This debate, according to Vale, had two ends: on the one hand, most commentators will always condemn civil defense planning as inadequate, and on the other, such planning can be censored… for representing an excess of state control. The concept of civil defense is controversial because it is inherently political and because it forces the choices of the state and the needs of private actors. But it is also controversial because of how some of the historical examples of the practice played out in the politics of the time. Civilian defense in the past has also been a concept used by dictators to justify "death squads" or other extrajudicial killings.

Let's go back to today's meaning of the term civil defense, or at least to the meaning that civil defense had it at the end of the Cold War:

- An organized defensive measure by civilians and/or the state to protect the civil population in times of war or other emergencies, such as natural disasters;
- Civil actions in support of military defense and military objectives;
- Actions of civilians in opposition to the state to protect the people from abuses of the state (self-defense);
- Actions "to alleviate the losses, damages and suffering caused to civilians as a result of the dramatic development of the means and methods of warfare. It is an essential component of the protection of civilians from military operations provided for by international humanitarian law" (ICRC 2021).

In our case, the focus is on the activities covered by the fairly broad definition in the Oxford Dictionary, where civil defense is defined as the following: "The organization and training of ordinary civilians to protect themselves from attack in wartime (or in the US, from natural disasters such as hurricanes)". At the root of this meaning, civil defense is as much about the psychological responses and resilience of the general population and the economy of the private sector as it is about the civil sector's direct contribution to warfare. This definition does not exclude measures involving civilians in support of military responses by the state.

3. THE CHALLENGE FOR CYBER CIVIL DEFENSE

The assumption among military analysts, cyber security experts, government security analysts and even managers of large private corporations in many countries is that a catastrophic peacetime cyber emergency is unlikely, but there is no agreement on what priorities regarding harmonization of planning of national strategies that such a situation might arise. The need to plan for extreme cyber emergencies is not only driven by the usual directives of the national defense policy, but also the unique characteristics of cyberspace and attack vectors or system failure in advanced cybernetic systems. The need has also been fueled by recent attention to hybrid warfare, particularly hostile acts that could not be categorized at the level of armed conflict as defined by the International Law of War (Humanitarian Law) and other sources of the law of war and the peace. Hence the need to review the history of the idea of cybernetic defense that would be carried out by civilians, i.e., cybernetic civil defense.

In 1998, the Defense Advanced Research Projects Agency (DARPA) launched its first network security project in terms of critical infrastructure resilience (Baumard 2017, 48). Also in 1998, society took the first steps towards possible collective preparations for joint civil defense when the UN General Assembly supported the resolution on development in the field of information and telecommunications in the context of international security. The same year, cyber

security was placed on a long list of things to be approved for bilateral development by Presidents Clinton and Yeltsin. After the terrorist attacks of September 11, 2001, the national security system was reformed in the United States with the creation of the National Homeland Security Agency and the Department of Homeland Security, which, among other things, were charged with new and broad responsibilities for cyberspace and the protection of critical information infrastructure (Hart 2001).

By 2003, the Ministries of Justice and Home Affairs of the G8 countries had adopted the Principles for the Protection of Critical Information Infrastructures (G8 2003). The principles can be seen as an affirmation of the need for classical cyber security at the enterprise level, but they go much further into the traditional realms of civil defense, even though that term is not clearly used. The principles are based on the fact that the responsibility for protecting critical information infrastructures is at the national level. This entails identifying threats across the country, reducing vulnerability, minimizing harm, encouraging rapid resilience and criminal prosecution investigations. The measures should include "communication, coordination and cooperation nationally and internationally among all stakeholders – industry, academia, the private sector and government entities, including infrastructure protection and law enforcement agencies". In the document, the protection of privacy and continuous security of sensitive information are placed as guiding directions.

By 2005, the US government had committed to a six-point plan to protect the applied Software applications for industrial process control (SCADA) from terrorist attack that included the following elements (Purdy 2005):

1. Establishing a National Cyber Space Response System for prevention, detection, response and rapid reconstitution after cyber incidents;
2. Cooperation with public and private sector representatives to reduce vulnerabilities and minimize the severity of cyber-attacks;

3. Promoting a comprehensive awareness plan to empower the entire population to secure their own parts of cyberspace;
4. Fostering appropriate training and education programs to support the nation's cyber security needs;
5. Coordinating with the intelligence and law enforcement communities to identify and mitigate cyber threats; and
6. Building a world-class organization that will aggressively advance its cyber security mission and goals in partnership with its public and private stakeholders.

In 2009, the Department of Homeland Security (DHS) made major policy changes by devising a ten-point plan for cyber resilience (DHS 2009) and offering corporations across the country a service called the Cyber Resilience Review (CRR) based on ten elements: Asset Management; Controls Management; Configuration and Change Management; Vulnerability Management; Incident Management; Service Continuity Management; Dealing with Risks; External Dependency Management; Training and Awareness; and Situational Awareness. This process was mostly oriented to the enterprise level, as well as towards classically defined technical aspects of cyber security, but it remains of lasting importance to the national level policy of preparedness for Critical Information Infrastructure Protection from cyber assault (complex cyber emergencies cases on a national scale).

In 2011, US President Barack Obama signed the Presidential Policy Directive PPD-8 on National Emergency Preparedness, including a nationally significant cyber-attack. In both 2015 and 2016, President Obama twice declared a national cyber emergency requiring dramatic changes in the US preparedness. Obama also issued a Policy Directive on National Coordination of Cyber Incidents (White House 2016). Confirmation that radical changes are taking place in the protection of critical information infrastructure came in May 2017, when President Trump signed a Presidential Executive Order to Strengthen the Cyber-security of Federal

Networks and Critical Infrastructure (White House 2017). In some ways, Trump's order was a declaration of war on the technological and procedural gridlock of the nation's cyber-security establishment. The order led to a shift in the public/private balance in the CIIP: It is an executive branch policy to use its authority and capabilities to support the cyber security risk management efforts of owners and operators of the nation's critical infrastructure. The order called for special attention to the electric power sector, asking the agencies to study the following: the potential scope and duration of an extended power outage associated with a significant cyber incident against the US electric subsector; the readiness of the United States to manage the consequences of such an incident; and any gaps or deficiencies in the assets or capabilities needed to mitigate the consequences of such an incident. It also calls for an assessment of defense war-fighting readiness through an additional study of "cyber security risks facing the defense industrial base, including its supply chain, and the platforms, systems, networks, and capabilities of the U.S. military as well as recommendations to mitigate these risks".

During this same period, the Pentagon undertook major reviews of its national security strategy and related military doctrine, based in part on an assessment of serious cyber threats to the United States. In the new National Security Strategy (NSS) that was issued in December 2017, its Pillar 1 (Homeland Defense) dealt more with "keeping America safe in the cyber age" and included measures already emphasized in the Executive Order (by the President). The National Security Strategy broadly described the importance of the population at large in ensuring national cyber resilience in extreme contingencies.

This legal treatment of cyber security is lacking in most countries in the world. In the US, the Cyberspace Operations update replaced the 2013 publication and provided new guidance for command and control of cyberspace operations and their planning. One of the big changes is the distinction between two modes of command and control for cyberspace operations: "routine and contingency/crisis". An important feature here for the U.S. allies is the recognition that a military

cyber-space alliance will look and function differently than other forms of cooperation, that is, "the level of integration of U.S. cyber-space forces with foreign cyber-space forces will vary depending from the individual agreements with each of those partners and may not reflect the level of integration with other types of forces" (JCS 2018). The Homeland Defense update recognizes the Cyber Command's role in homeland defense missions, and assigns the Special Operations Command primary responsibility for coordinating cyber missions against terrorists on US soil. It also positively declares a new mission of coordinating with the private sector for homeland cyber defense operations involving the US military (Austin 2019, 19).

On the international stage, although the UN resolution related to the above and first introduced in 1998 had a confirmed and politicized history that included occasional clashes between the two cyber blocs (the US and its allies against China, Russia and their like-minded countries), the resolution finally led to a consensus in 2015 in the Group of Governmental Experts (GGE) on possible voluntary norms regarding common civil defense measures in cyberspace. In general, the essence of the voluntary norms is that the state should not implement or encourage information and communication technology activities contrary to international law, which would intentionally damage the critical infrastructure for providing services to the public; the state should not allow a cyber infrastructure to operate on its territory under the authority of its government that would unlawfully act on other states; states should take all measures to protect their critical infrastructure from threats from information communication technologies; states should encourage responsible reporting of ICT vulnerabilities and sharing of related information about available remedies for such vulnerabilities (Austin 2019, 19).

The International Atomic Energy Agency (IAEA) in 2012 and the International Civil Aviation Organization (ICAO) in 2017 each took important initiatives in their own area for the protection of critical information infrastructure. In the case

of ICAO, it should be noted that the members previously supported a new treaty (the Beijing Convention) in 2010 which, among other things, criminalized "technological attacks" on aircraft or air traffic control (Austin 2019, 20).

Some leading private sector organizations have also begun to give high priority to planning for extreme cyber emergencies. According to a 2013 survey, conducted by the World Federation of Exchanges (WFE) and the International Organization of Securities Commissions (IOSCO), cybercrime in securities markets can be considered a systemic risk. According to the report of the US President's National Infrastructure Advisory Council, the country has failed in its mission of protecting critical information infrastructure. Although the report criticizes, it nevertheless points out with hope that cyber civil defense is credible and feasible, that is, the Council (NIAC) believes that the federal government and the private sector collectively have the vast cyber capabilities and resources needed to defend critical private systems from aggressive cyber-attacks - if they are properly organized, controlled and focused (NIAC 2017, 5). It is quite debatable whether other countries also enjoy this confidence. For example, a 2018 survey of more than 400 companies worldwide, conducted by the Economist Intelligence Unit, found little consensus on resilience measures and planning, underpinned by a pervasive lack of confidence in the availability of all the people needed to contribute to outcomes (Insurance Journal 2018).

There is some research that suggest that all countries, including major powers such as France, China, India, Russia, Israel, the United Kingdom and Australia, face similar shortcomings in cyber civil defense due to similar reasons related to technological vulnerability and the late onset of corrections in national cyber security policies (Austin 2019, 20).

Shen speaking of this issue, China, a rising cyber power but far weaker in cyber defense than the United States, has moved with considerable speed, starting in earnest in 2015, staking its national security vision on cyber security. President

Xi has said that "there can be no national security without cyber security" and regarding the country's 2015 military strategy, that "outer space and cyberspace are the new commanding heights of the entire international security competition". These statements imply that the key states see existing gaps in cyber civil defense as significantly influencing the strategic policy. They believe that such a gap will limit highly vulnerable countries with little ability to respond in shaping coercive pressure on potential adversaries. Countries that are less vulnerable in cyberspace, such as North Korea, may be more emboldened for aggressive action (Austin 2019, 19).

Between 2015 and 2019, there was a tectonic shift in the urgency and character of civil defense planning for cyber-attack in several countries. We have now reached a point where the largest cyber powers in the world are publicly declaring that it is an arms race. These statements stem from findings that states' civil defenses in cyberspace are not only seriously deficient, but that these deficiencies can be remedied in a way that contributes to the overall strategic power and military deterrence (of the United States). The idea of "international" information infrastructures is already underway with the work of the Global Commission for the Stability of Cyberspace (GCSC), which tends to protect the core (main servers) of the Internet. As early as 2007, the US government became concerned about such international dependencies in a range of critical infrastructures, including ICT-related ones, and set up the Critical Foreign Dependencies Initiative (CFDI). As part of this process, the US government has asked its embassies to report those facilities in their host country that may be considered critical to the US national security or economic prosperity. Based on the responses, the Department of Homeland Security compiled a prioritized list of these dependencies that included "over 300 assets and systems in more than 50 countries" (DHS 2008).[37)]

[37)] In many cases, land stations on undersea cables in foreign countries, as well as other telecommunications infrastructure, were involved.

INSTEAD OF A CONCLUSION: PROBABILITY OF A CYBER-ATTACK AND CAPACITIES FOR PROTECTION OF THE INFORMATION INFRASTRUCTURE

By the end of the first decade of this century, awareness grew that attacks on critical information infrastructure could eventually cause serious economic shocks, definitely at the national level and possibly at the international level. As part of the OECD's series of five case studies on the potential for global shocks, a report on whether such a shock could be triggered by a cyber-attack was produced. The conclusion is that very few isolated cyber events have the capacity to cause a global shock and that "It is unlikely that there will ever be a true cyber war", assessing that deterrence in cyberspace is not really operational at the strategic level of a conflict. This assessment is based in part on the ability of systems to withstand cyber-attacks without additional assistance and the ability to defeat cyber-attacks with good planning (Sommer and Brown 2011, 6).

In 2013, Thomas Rid published his book "Cyber War Will Not Take Place". His primary thesis is that: "cyber war", independent of the non-cyber domain, is quite unthinkable, since any war is an act involving political, economic and civilian resources of states, as well as their military technological resources, both non-kinetic (including cyber) as well as kinetic (including bombs and missiles) (Rid 2013). Reed's thesis has often been misinterpreted to mean that a war based on ICT dominance and cyber warfare was some kind of exaggeration. Several studies by the RAND Corporation contributed to this, pointing out that cyber weapons could not achieve a result at a strategic level in war.

An article by Kello (2016) looks at the problem from one key perspective: "the possible strategic and other consequences of arming civilian segments of cyberspace with active defensive capabilities". His article is based on the globally accepted reality that states cannot adequately protect their private corporations, including critical infrastructure, in cyberspace.

Lewis (2018) in his monograph correctly assesses the main source of threat to states from large-scale disabling cyber-attacks rather than from criminals or terrorists. At the same time, the book's focus is on the likelihood of such an attack, seeing it as low. But as the likelihood diminishes, Lewis seems to diminish the importance of contingency planning for such an event. The paper does not analyze the appropriate response of states at all, because it is considered normal for states, especially in the West, to have contingency plans for very unlikely events, including nuclear war, mass terrorist events, or major natural disasters. Overall, the global impact of several significant cyber-attacks, particularly theft and the release of malware, has been underestimated.

REFERENCES

1. Austin, Greg. 2019. "Civil Defence Gaps Under Cyber Blitzkrieg". *Discussion Paper No 6*, UNSW Canbera.
2. Austin, G. and Sharikov, P. 2016. "Pre-emption is victory: aggravated nuclear instability of the information age". *The Nonproliferation Review* 23(5-6) 691-704
3. Baumard P. 2017. *Cybersecurity in France*. Cham: Springer International Publishing AG
4. CISA. 2018. "*Cyber Storm Final Reports*". Accessed May 22, 2022. https://www.cisa.gov.
5. DHS. 2008. "Fact Sheet: Critical Infrastructure and Homeland Security Protection Accomplishments". *Department of Homeland Security, 5 September 2008*. https://www.hsdl.org.
6. DHS. 2009. "Cyber Resilience Review". *Department of Homeland Security*. https://www.us-cert.gov.
7. G8. 2003. Principles for the Protection of Critical Information Infrastructures. May 2003. http://cybersecuritycooperation.org.
8. Hart Rudmann. 2001. "Road Map for National Security: Imperative for Change". *The Phase III Report of the U.S. Commission on National Security/21st Century. The United States Commission on National Security/21st Century*. 15 February 2001. http://www.au.af.mil.
9. ICRC. 2021. "Civil Defence in International Humanitarian Law". *Advisory Service on IHL*. Geneva: ICRC, April 2021.
10. Insurance Journal. 2018. Most Global Organizations Fail to Learn from Cyber Mistakes: WTW Survey. June, 22, 2018. Accessed March, 14, 2022. https://www.insurancejournal.com.

11. JCS. 2018. "Cyberspace Operations. JP 3-12". *Joint Chiefs of Staff*. https://www.jcs.mil.

12. Kello, L. 2016. Private-Sector Cyberweapons: Strategic and Other Consequences. 15 June 2016. http://dx.doi.org.

13. Lewis J. 2018. *Rethinking Cybersecurity: Strategy, Mass Effect, and States*. CSIS. https://csis-website-prod.s3.amazonaws.com.

14. NIAC. 2017. "Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure". *The President's National Infrastructure Advisory Council*. https://www.dhs.gov.

15. Oxford Learner's Dictionaries. Definition of civil defece noun. Accessed May 12, 2022. https://www.oxfordlearnersdictionaries.com.

16. Pescaroli G. and Kelman I. 2017. "How critical infrastructure orients international relief in cascading disasters". *Journal of Contingencies and Crisis Management* 25(2) 56-67. https://onlinelibrary.wiley.com.

17. Purdy A. 2005. "Prepared Statement. Joint Hearing before the subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity with the Subcommittee on.

18. Emergency Preparedness, Science, and Technology of the Committee on Homeland 109th.

19. Security". *House of Representatives Congress. First Session*. 18 October 2005.p9.

20. https://pdfs.semanticscholar.org.

21. Rid T. 2012. "Cyber War Will Not Take Place". *Journal of Strategic Studies*. 35:1 5-32. https://doi.org.

22. Sommer P. and Brown I. 2011. "Reducing Systemic Cybersecurity Risk". *OECD*.

23. *FP/WKP/FGS (2011)*.

24. Stacey, B. 2015. Statement of Mr. Brent J. Stacey, Associate Laboratory Director National & Homeland Security Idaho National Laboratory before the United States House of Representatives Science Subcommittee on Energy and Science Subcommittee on Research and Technology, 21 October 2015.

25. Sukjenik, Konstantin. 1976. *Civilna odbrana stranih zemalja*. Beograd: VIZ.

26. Vejl, Lorens Dž. 1991. *Civilna odbrana. SAD, Švajcarska, V. Britanija, SSSR*. Beograd: VINC.

27. White House. 2016. PPD 41, President Policy Directive: United States Cyber Incident Coordination, July 2016. https://obamawhitehouse.archives.gov.

28. White House. 2017. "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure". May 11, 2017. https://trumpwhitehouse.archives.gov.

Jelena Dinić*)

UDC: 35.07:005.334
351.78:711.42

URBAN RESILIENCE IN THE ERA OF UNCERTAINTY: REFLECTIONS ON LOCAL GOVERNANCE AND SOCIAL MEMORY

Abstract: *Resilience of urban communities is a complex phenomenon that requires holistic and multidisciplinary approach. In the scientific literature, this phrase is presented through the prism of cascading capacities embodied in the ability of the urban system to adequately respond to stressors, adapt to new operating conditions and recover as soon as possible, while preserving vital functions and identities. The economic, social, environmental and institutional spheres form the basic, interdependent dimensions of resilience and the basic structure for further operationalization of the resilience of urban communities. Institutions have an integrative role within the system of urban communities, giving the necessary impetus to actors operating at several different levels. The authority and legitimacy of institutions in democratic societies is based on the will of the citizens expressed in the elections. The representative role of institutions based on the mentioned processes gives them the power to decide and influence vital parts of the system. Institutions also have the resources to initiate and accelerate complex process of building resilient urban communities. Stressors play a constructive role as they encourage communities to deve.lop and change, representing a transformative factor in the process of creating a resilient urban community. The adaptive capacity of urban communities largely depends on collective learning, based on past experiences, and as such is a derivative of the social dimension of resilience. Most prominent scholars agree that urban communities can never return to the state of the system that existed before the experience with a certain form of security threat due to the process of collective learning and memory. Using case studies and a qualitative content analysis of the available documentation, the author will describe and explain the impact of governance and social memory processes on building resilient urban communities in an era of dynamic change and uncertainty.*

Key words: *urban communities, resilience, institutional governance, social memory, uncertainty.*

*) PhD candidate, Faculty of Security Studies, University of Belgrade

INTRODUCTION

The resilience of urban communities is a complex, multi-layered phenomenon that can be explored through the implementation of top-down and bottom-up approaches. For the purpose of writing the present paperwork, both approaches were used in order to assess the role of institutional factors and social memory in the process of building resilience of urban communities to the various forms of security threats in the era of dynamic changes and uncertainty.

Institutional actors have great potential in the form of mobilizing and directing resources within the system, as well as developing long-term strategies that give significant contribution to the process of building resilient urban communities. This paper presents case studies with empirical support to the importance of local governance in the process of strengthening community resilience capacities.

Social memory is a derivative of the psycho-social dimension of resilience. Learning as one of the basic components of social memory can be manifested through proactive processes in the form of risk awareness and preparedness or reactively, through learning from experience with a certain stressor that affected security and the overall system functioning.

As part of the analysis, the presented case studies illustrated the importance of institutional governance and social memory in the process of building resilience of local communities.

1. THE ROLE OF LOCAL GOVERNANCE IN THE PROCESS OF BUILDING RESILIENT URBAN COMMUNITIES

In democratic societies, legitimacy gained through elections gives institutions the leverage to foster transformative change and build resilience through a wide range of activities (Lostrangio 2020; Chaffin and Schown 2017). According to some authors (Bristow and Healey 2014), institutions play the role of connectors

within the urban community system, providing collective meaning to individual actions. Representative power and institutional resources provide an additional impulse towards the development of long-term strategies and legislative acts facilitating urban community resilience (Lang 2012).

Institutional changes are the essential element in generating multi-layered, polycentric structures leading to transformation and the creation of resilient urban communities (Pisano 2012). Some authors (Djalante et al. 2011) believe that community resilience is based on adaptive governance including multi-level polycentric institutions, participation and cooperation of citizens, self-organization, networking, political and social learning, as well as institutional memory. Institutions with adaptive attributes have the capacity to deal with uncertainties and rapid changes (Carpenter et al. 2012).

The period of time immediately after the system is confronted with a certain type of stressor is particularly delicate because the coordinated action of numerous institutional and wider social actors was required. Some authors have used the Stage VI Turner model to explain in detail the synergistic effect of resilience and governance within a certain cultural concept (Gajendran 2017). The essential characteristics of the said concept are reflected in uncertainties, difficulties in establishing control, power relations, interests; adaptive governance precedes the resilience of the system as the ultimate outcome and must have reformative features and the implementation of innovative solutions (Gajendran 2017, 4).

According to Welsh, institutional governance is used as a discourse on human security in a complex networked world, shifting the focus from the state bodies to the society and community (Welsh 2014, 19). The basic characteristics of resilient systems, embodied in adaptability, flexibility and functional continuity, are implemented mainly in security strategies related to emergency response (Welsh 2014). The main goal of building resilience within the framework of institutional management is to enable institutional actors and individuals to respond to internal and external stressors (Welsh 2014). The cascading capacities

of resilience embodied in the process of prevention, response and recovery are used as a framework for the development of documents related to response in emergency situations.

1.1. RISK GOVERNANCE AND COMMUNITY RESILIENCE

The outstanding complexity, uncertainty and interdependence between numerous actors at different levels and distances pose a challenge for understanding the processes between local and global structures (Wilbanks 2007). Some scholars (Carabine and Wilkinson 2016, 64) determined the characteristics of institutional risk management at the local level through the prism of socio--ecological system theory. The inclusion of a large number of different actors in the decision-making process, polycentricity, flexibility, decentralization, participation and the inclusion of citizens in the decision-making process, are essential for communities that strive to build resilience attributes (Wilkinson 2016, 64).

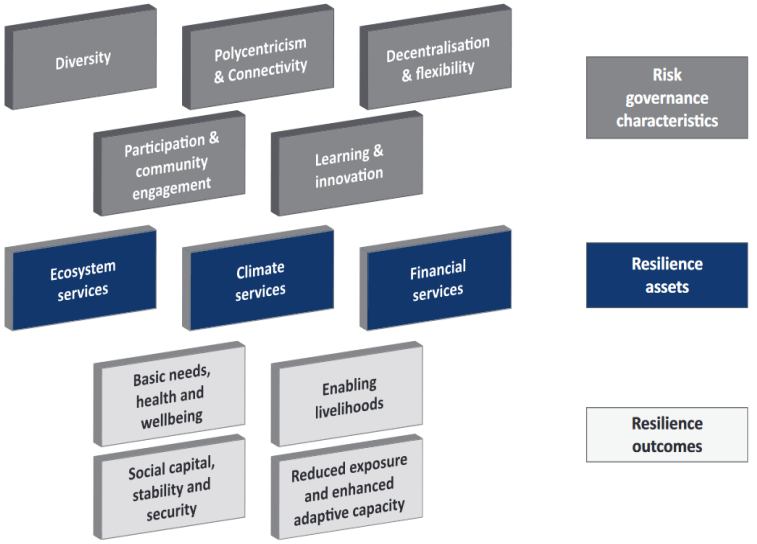


Figure 1 – Conceptual framework representing the link between risk governance and resilience as outcome (Carabine Wilkinson 2016, 64)

Uncertainty as a product of the dynamics of global events requires the ability to adapt to all relevant actors at the local level. According to Gunderson and Holling (2002), learning from mistakes and introducing innovations are very important processes that contribute to strengthening institutional memory and allow mistakes from past experiences not to be repeated.

A branch of executive authorities that makes an outstanding contribution to building resilient communities are the first responders (police, fire-rescue units and ambulance). By illustrating the Emergency Management Lifecycle, a deeper insight is gained into the contribution of the aforementioned services in strengthening the capacity of the community in response to various forms of hazards.

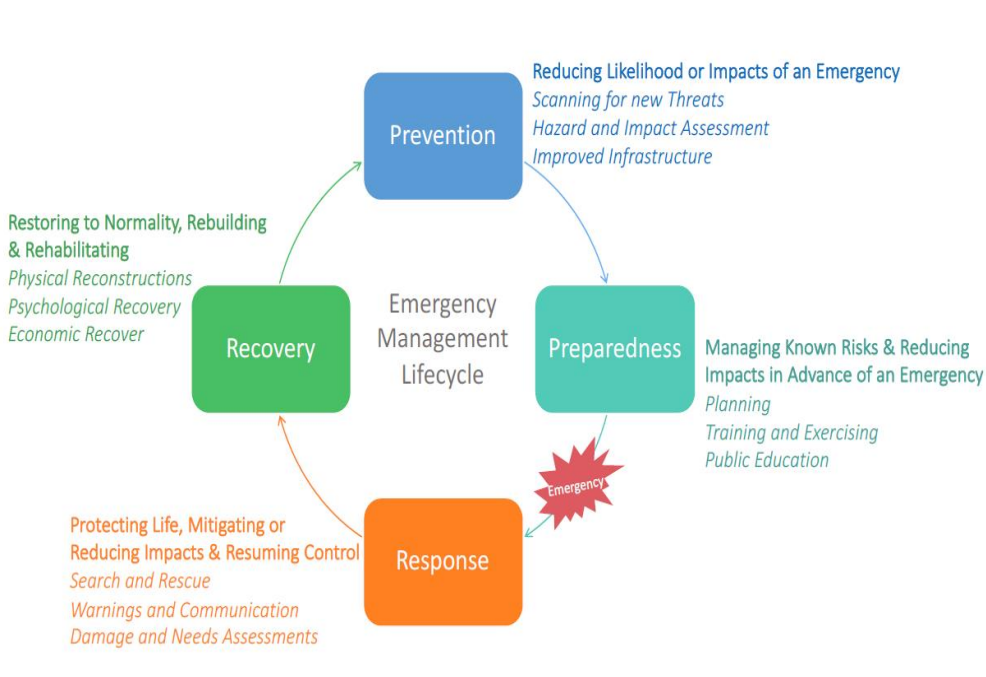


Figure 2 – Emergency management lifecycle according to the UK's approach in emegency situations (Parsons 2019, 2)

1.2. LOCAL RESILIENCE FORUMS IN UK

A particularly important concept aimed at encouraging the development of resilient communities was very successfully applied in local communities in the United Kingdom. Local Resilience Forums (LRF 2022) are a mechanism for achieving the resilience of urban communities in the UK, and their existence is governed by the Civil Contingencies Act. They were established in 2004 with the aim of facilitating interaction between stakeholders such as police, EMS, firefighters, local authorities, government agencies and actors involved in decision-making and emergency response (Fisher et al 2015).

In 2019, the UK government adopted the document named "The role of LRF", which clearly defined the criteria for self-assessment of work and progress in operation. Certain authors give a critical review of the LRF activities due to the fact that the public has limited access to information regarding their work. Performance of LRF is not under the normative framework of the Freedom of Information Act because they do not have the status of public bodies (The role of LRF 2019).

The operation of the existing 42 LRFs is determined by the synchronous operation of first and second category responders (Cabinet Office 2013). First category responders include local authorities, police, fire and rescue units, emergency services and other associated services that form the basic lever for responding in emergency situations. Responders of the second category refer to public companies or a group of organizations, such as the Red Cross, that provide support to responders of the First Category in the form of cooperation and provision of information in order to provide a better response to emergency situations in local communities.

Category 1 organisations	
Local authorities	All principal local authorities
Government agencies	Environment Agency, DEFRA, Maritime and Coastguard Agency
Emergency services	Police forces, British Transport Police, fire authorities, ambulance services
Health services	Primary care trusts, Health Protection Agency, National Health Service Acute Trusts (hospitals), foundation trusts, port health authorities
Category 2 organisations	
Utilities	Electricity, gas, water and sewerage, public communications providers (landlines and mobiles)
Transport	Network Rail, train operating companies (passenger and freight), Transport for London, London Underground, airports, harbours and ports, Highways Agency
Government	Health and Safety Executive
Other	Chamber of commerce, non-governmental organisations and social care charities

Table 1 – Category 1 and Category 2 organisations included in perfomance of LRF in UK (Fisher and Chmutina 2014, 95)

According to the document "The Role of Local Resilience Forums", the main purpose of LRF is to ensure Category 1 responders to addres all aspects of policy in relation to "risk, planning for emergencies, planning business continuity management, publish information about risk assesment and plans, arrangements to warn and inform the public, other aspects of civil protection duty and support for the preparation of multi-agency plans and other documents" (Cabinet Office 2013:10).

The engagement of a large number of stakeholders from different activities and jurisdictions contributes to strengthening the individual capacities of the community and building comprehensive resilience. On an empirical level, LRF made a significant contribution during major floods in Great Britain 2013 through the process of informing the public about the emergency situation and instructions for citizens' actions. By using social networks as a channel for informing the general public, LRF contributes to situational awareness and effective response to emergency situations in the local community (Bunney et al. 2018). A particularly important segment in informing the public through social networks Twitter and Facebook refers to the possibility of removing misinformation and misinterpretations by the general public (Bunney 2018, 322).

1.3. THE ROLE OF SOCIAL NETWORKS IN THE PROCESS OF BILDING COMMUNITY RESILIENCE IN UK

A certain number of researchers make a critical review of the reactive and passive presence of LRFs on social networks, considering that LRFs should use their full potential in communicating with a wide audience (Meaton and Stringer 2013). The findings of a multimethod research regarding social networks usage by first responders during emergency situations in the UK (Parsons 2019) indicated the importance of social networks in improving citizens' preparedness for responding to emergency situations and building resilience in response to a wide range of hazards. A significant finding of the research refers to the sense of belonging and empathy that was developed among users who downloaded information from first responders through social networks (Parsons 2019,185).

The presence of institutional actors on social networks opens up a number of possibilities in the process of building resilient social communities. According to Parsons (2019,171-172), it is necessary to implement a set of measures in order to mobilize the full potential of social networks and their positive impact on emergency management in UK:

- Provide additional financial resources, intensify governance in the direction of institutionalizing the use of social networks, policies and plans for management in emergency situations;
- Feasibility assessments and regular revision of logistics are necessary; the great pressure to which first responders are exposed should not be further increased by engagement on social networks during emergency situations;
- Identify employees with knowledge of social networks who will be in charge of the organization's activities on online platforms; their duties within their job description must be clearly highlighted;

- Provide periodic training so that employees are informed about the development possibilities of social networks, especially the technical changes that are incorporated by social network providers;
- The organization of demonstration drills should be accompanied by social networks notifications;
- Strategies for the social networks usage by first responders should be aimed at reaching a wider audience that will be encouraged to take part in the activities; the usage of videos and photos is recommended as an incentive for citizens to participate in emergency situations;
- Feedback from citizens regarding the usage of social networks is extremely important; the use of questionnaires can provide valuable insights into segments that should be improved.

	Key Objectives (KO)		
	A: Preparedness & Resilience Building	*B: Relationship Development*	*C: Emergency Communications*
Desired Outcomes (DO)	1: Audience Engagement 2: Social Influence 3: Behaviour Change 4: Raised Risk Awareness	1: Audience Engagement 5: Public Trust 6: Increased Organisational Awareness	1: Audience Engagement 7: Large Public Reach 8: Informed Audience

Table 2 – Key objectives and desired outcomes of social media usage by first responders in UK (Parsons 2019, 93)

1.4. INSTITUTIONAL GOVERNANCE AND COMMUNITY RESILIENCE – A CASE STUDY: COVID-19 PANDEMICS IN IRAN

Institutional governance is one of the essential elements in establishing a resilient society in conditions of uncertainty generated by global changes. Based on a case study conducted in the Iranian city of Trabiz, a group of scientists tried to answer the research question: which elements of institutional management influenced the promotion of community resilience in the face of the risks of the *Covid-19* pandemic in the Iranian city of Trabiz (Heidari et al. 2022).

Urban communities face a large number of threats arising as a result of natural forces or human activities with destructive potential on the overall functioning of society. As part of the mixed design study, the Delphi method was used with the participation of 15 experts from the field of urban planning who managed the selection of indicators of institutional governance aimed at establishing resilient urban communities. The set of mentioned indicators refered to participation, transparency, legitimacy, justice, responsibility, reliability, efficiency, effectiveness, consensus and flexibility (Heidari et al 2022, 2).

Research findings indicated high scores of participation, responsibility, reliability as key elements in building a resilient urban community in the face of the *Covid-19* pandemic (Heidari 2022).

2. SOCIAL MEMORY AS SOCIETAL DIMENSION OF RESILIENCE

The resilience attributes are reflected through “the existence, development and engagement of community resources by its members to thrive in an environment characterized by change, uncertainty, unpredictability and surprise” (Magis 2010, 402). Community resilience is made up of numerous inseparable dimensions that

can be explored through many different levels of analysis. The idiographic (bottom-up) approach is applied in order to consider human and social drivers as predictors of the resilience of urban communities (Wilson et al. 2018).

In the scientific literature, social memory is a derivative of the societal dimension of resilience and includes social learning from previous experiences, traditions and customs (Wilson 2018). According to Folke (2006), social memory plays very important role in building resilience of social communities due to the fact that they accumulate practices, knowledge and values of individuals and institutions and thus prepare the community for the process of building resilience and facing numerous uncertainties. In the context of social memory after facing a certain type of stressor, "the past becomes the present and thus creates the potential for action" (Beilin and Wilkinson 2015, 5).

Scholars make a distinction between natural and human systems in the context of community resilience (Wilson 2008, 5). Natural systems have systemic memory and do not have anticipatory mechanisms, while human systems are anticipatory, non-deterministic and within their framework, social memory leads to learning and adaptation based on previously acquired experience (Wilson 2008, 5).

Social memory has the greatest influence on adaptive capacity, i.e. the ability to adapt social factors to new circumstances after experiencing a certain type of hazards such as fires, floods, earthquakes. One of the most important components of social memory is social learning (Wilson 2013). The adaptive capacity of a community is highly dependent on the lessons learned from the past experiences, implemented in innovative strategies aimed at building resilient communities (Keen et al. 2005).

Researchers from specific scientific disciplines, such as human geography and political ecology, have highlighted the importance of social memory in the context of understanding the resilience of communities (Wilson 2013). The previously

conducted studies (Folke 2003, Wilson 2013, Tidball et al. 2010) investigated the impact of the memory of individuals and stakeholders on the community's ability to adapt to changes caused by various disturbances in the system (Wilson 2013, 231).

According to Wilson (2013, 235) and Davidson (2010), learning is a complex process that includes customs, interpretations of information at the individual or collective level, group discussions, imagination and anticipation of events. A particularly important component in the learning process is proactive learning that contributes to the positive quality of the process itself (Cutter et al. 2008) which, due to its non-linear nature, requires constant adjustments, especially in the way of passing on experience to future generations. Some researchers believe that only a partial transfer of knowledge between generations is possible (Olic and Robins 1998), and that each generation must experience similar stressors in order to be able to learn certain lessons. In order for a certain community to have the attribute of resilience, it is necessary for learning to have a transformative component, that is, to separate useful experiences through selective mechanisms and thereby strengthen the adaptive capacity (Wilson 2013, 237). According to Lebel (2006), hiring external experts can lead to weakening of the endogenous adaptive capacity. The involvement of the entire community is essential for the process of learning and building a resilient system. The method of intergenerational transmission of knowledge constitutes an essential link in the process of social learning, especially in the form of the tradition of oral transmission of knowledge and experiences in the community. Time distance in relation to the period in which the security of the community was in some way threatened can lead to a distorted perception of risk and affect the adaptive capacity of future generations (Wilson 2013, 238). With emigration or generational change of community residents, "cracks" are created in social memory. By strengthening traditions and customs in the community, as well as the sense of belonging that develops through longer residency in the community, a cohesive force is created that improves social memory and overcomes the previously mentioned weaknesses (Wilson 2013).

The uneven distribution of power, present in every community, has a significant impact on the process of social learning, because certain groups have access to resources (such as modern technologies, information or finance) that are denied to a larger number of social groups (Wilson 2015). Economic, political, immigration or leadership changes lead to changes in historical stakeholder networks and indirectly affect the changes in community customs and traditions (Wilson 2015, 241). Demographic changes in the form of young people emmigration significantly reduce the social capital and the adaptive capacity of the community becoming vulnerable (Wilson 2013). By facing new hazards, the process of restoring the lost social memory created by the emmigration of the young generation from their native areas can be initiated.

An insight into the oral traditions of individual nations illustrates examples of the positive impact of social memory on community resilience. The residual memory of the tsunami that hit the Indonesian island of Sumatra and killed more than 70% of the population in 1907 had the positive effect reflected in 2004 tsunami when the number of victims was reduced to 1% of total population (Wilson 2015, 242; Gaillard et al, 2008).

Social memory can also have a negative impact on community vulnerability. Autocratic societies with power imbalances have a destructive impact on community resilience (Wilson 2012). Manipulation of information by elites in areas with pronounced land desertification negates social memory in order to obtain profits and accumulate power (Wilson 2015, 243).

By investigating the "input" of social memory into new communities through immigration flows, researchers have come to the conclusion that one to two generations of new community members possess residual social memory in new environments as well (Ward and Styles 2006; Neal 2009). According to Wilson (2015), adapting to the traditions and customs of the new environment is an essential element on the way to building resilient societies.

2.1. SOCIAL MEMORY AND BUILDING COMMUNITY RESILIENCE – A CASE STUDY: EARTHQUAKE IN CHRISTCHURCH, NEW ZEALAND

The strong earthquakes in New Zealand in 2010 opened up space for researchers to investigate the impact of social memory on the process of recovery and building a resilient urban community after the aforementioned disaster. The complex process of social memory (Olic and Robins 1998) affects the ability of a community to adapt to a certain type of disaster through accumulated knowledge, experiences and skills residing in people, institutions and places (Wilson 2013, 208).

Researchers have highlighted the distinction between individual and collective resilience while analyzing the Christchurch earthquake. Individual residents demonstrated resilience after the earthquake in contrast to the entire community, which was faced with scandals due to the city authorities' indecision in dealing with the consequences of the disaster (Wilson 2013, 210). Using qualitative techniques, the researchers came to the conclusion that the difficulties in building the psycho-social component of community resilience were the results of the absence of disasters throughout history that would trigger the process of social memory (Wilson 2013).

Christchurch residents did not undertake proactive learning based on preparedness and risk assessment but relied on reactive learning in the post-disaster recovery process (Cutter 2008). The absence of preventive measures, as well as reparation activities immediately after the disaster, led researchers to the conclusion that Christchurch was a negative example of social memory and adaptation (Davidson 2010; Wilson 2013).

CONCLUSION

Tectonic changes in the global arena require development of transformative and adaptive mechanisms of actors at different levels. In the time of extremely complex changes, resilience was imposed as a paradigm with the potential to mitigate and overcome the negative consequences arose as a result of the uncertainty that pervaded every segment of social reality.

Implementation of top-down and bottom-up approaches in assessing the resilience of urban communities is necessary in gaining in-depth insights into various aspects of the mentioned phenomenon. Looking at the attributes of resilience from a dual perspective, observing citizens and institutional actors point of view, minimizes one-sidedness in research efforts at the empirical level.

Coping with a particular stressor requires institutional responses at different levels. The establishment and functioning of the Local Resilience Forum in UK is one of the examples of good practice of building community resilience. The great potential of using social networks as a channel for the promotion of preventive activities of first responders, informing citizens about potential hazards and placing appeals for the mobilization of volunteers in the process of response and community reconstruction should be a guideline for strengthening institutional structures in the process of creating a resilient society.

The collective memory related to the response to various forms of past security threats is transmitted intergenerationally, and largely shapes the absorptive and adaptive capacity of society to deal with future stressors. Preservation of social memory is especially important in communities that face intense demographic changes in the form of immigration and emigration processes. Prioritizing proactive learning over reactive learning can further strengthen the preventive capacity of the community in an era of progressively increasing global uncertainties.

REFERENCES

1. Beilin, R., & Wilkinson, C. 2015. Introduction: Governing for urban resilience. *Urban Studies*, *52*(7), 1205-1217.
2. Bristow, G., & Healy, A. 2014. Building Resilient Regions: Complex Adaptive Systems and the Role of Policy Intervention. 72:93–102.
3. Bunney, S., Ward, S., & Butler, D. 2018. Inter-organizational resilience for flood focused emergency planning: examining multi-agency connectedness through Twitter. *Water Practice & Technology*, *13*(2), 321-327.
4. Carabine, E., & Wilkinson, E. 2016. How can local governance systems strengthen community resilience? A social-ecological systems approach. *Politics and Governance*, *4*(4), 62-73.
5. Carpenter, S. R. et al. 2012. Program on ecosystem change and society: An international research strategy for integrated social–ecological systems. *Current Opinion in Environmental Sustainability*, *4*(1), 134-138.
6. Chaffin, B., & Scown, M. 2017. Social-ecological resilience and geomorphic systems. *Geomorphology*, 221–230.
7. Cutter, S.L., L. Barnes, M. Berry, C. Burton, E. Evans, E. Tate and J. Webb. 2008. A Place-Based Model for Understanding Community Resilience to Natural Disasters. *Global Environmental Change*, 18, 596-606. https://doi.org.
8. Davidson, D.J. 2010. The applicability of the concept of resilience to social systems: some sources of optimism and nagging doubts. *Society and Natural Resources* 23:1135-1149.
9. Djalante, R., Holley, C., Thomalla, F., 2011. Adaptive Governance and Managing Resilience. *International Journal of Disaster Risk Science*, Volume 2, pages 1-14.

10. Fisher, J., Chmutina, K., Bosher, L. 2015. Urban Resilience and Sustainability: The Role of a Local Resilience Forum in England. In: Masys, A. (eds) *Disaster Management: Enabling Resilience. Lecture Notes in Social Networks*. Springer, Cham. https://doi.org.

11. Folke, C. 2006. Resilience: The emergence of a perspective for social-ecological systems analyses. *Global environmental change*, *16*(3), 253-267.

12. Folke, C., J. Colding and F. Berkes. 2003. 'Synthesis: building resilience and adaptive capacity in social-ecological systems', in F. Berkes, J. Colding and C. Folke (eds) *Navigating Social-ecological Systems: Building Resilience for Complexity and Change*. Cambridge: Cambridge University Press. pp. 329-352.

13. Gaillard, J.C., E. Clare, V. Ocean, D. Azhari, J.C. Denain, Y. Efendi, D. Grancher, C.C. Liamzon, D.R. Sari and R. Setiwan. 2008. 'Ethnic groups' response to the 26 December 2004 eruption and tsunami in Aceh, Indonesia'. *Natural Hazards* 47: 17–38.

14. Gajendran, T., & Oloruntoba, R. 2017. Governance and resilience: A case of re-development after a bushfire disaster. *Technological Forecasting and Social Change*, *121*, 50-64.

15. Gunderson, L. H., & Holling, C. S. (Eds.). (2002). *Panarchy: understanding transformations in human and natural systems*. Island press.

16. Heydari, M. T., Rasoulzadeh, Z., Hasanalizadeh, M., & Heshi, M. N. 2022. Explaining the Effects of Urban Good Governance on Citizens' Social Resilience against Covid-19 Epidemic (Case Study: Tabriz City). *Sustainable city*, *4*(4), 17-33.

17. Keen M, Brown V A and Dyball R eds .2005. Social learning in environmental management Earthscan, London

18. Lang, T. 2012. How do cities and regions adapt to socio-economic crisis? Towards an Instutionalist Approach to Urban and Regional Resilience. 70:285-291.

19. Lebel, L., J.M. Anderies, B. Campbell, C. Folke, S. Hatfield-Dodds, T.P. Hughes and J. Wilson. 2006. Governance and the capacity to manage resilience in regional social-ecological systems. *Ecology and Society*, Volume 11 (1), http://www.ecologyandsociety.org.

20. Local Resilience Forums. https://www.gov.uk.

21. Magis, K. 2010. Community resilience: an indicator of social sustainability. *Society and Natural Resources* 23 401-16

22. Maria C. Lostrangio. 2020. *How can local authorities plan for urban resilience? Co-creating and Orchestrating Multistakeholder Innovation*, Finnish University for Applied Science.

23. Meaton, D. J., & Stringer, L. A. 2013. The use of social media by UK local resilience forums. *WIT Transactions on The Built Environment*, *133*, 25-36.

24. Neal, S. 2009. Rural Identities: Ethnicity and Community in the Contemporary English Countryside. Aldershot: Ashgate.

25. Newham Council 2011 Quid pro quo, not status quo. Why we need a welfare state that builds resilience (www.newham.gov.uk).

26. Olick J K and Robbins J. 1998. Social memory studies: from 'collective memory' to historical sociology of mnemonic practices. *Annual Review of Sociology* 24 105-40.

27. Pisano, U. 2012. Resilience and Sustainable Development: Theory of resilience, systems thinking and adaptive governance, ESDN Quarterly Report No. 26.place-based model for understanding community resilience to natural disasters'. Global Environmental Change 18: 598–606. social-ecological systems'. Ecology and Society 11 (1), article no 19 [online]https://www.esdn.eu/fileadmin/ESDN_Reports/2012-September-Resilience_and_Sustainable_Development.pdf

28. Sophie Parsons. 2019. *The evolving symbiotic relationship between social media and emergency management: an exploration into the value of social media for emergency responders in UK*, University of Southampton.

29. The role of LRF https://assets.publishing.service.gov.uk.

30. Tidball, G.K., E.M. Krasny, E. Svendsen, L. Campbell and K. Helphand. 2010. 'Stewardship, learning and memory in disaster resilience'. *Environmental Learning Research* 16 (5–6): 591–609.

31. Ward C, Styles I. 2006. Evidence of the ecological self: English-speaking migrants' residual links to their homeland. *International Journal of Applied Psychoanalytical Studies* 4(4): 319-332.

32. Welsh, M. 2014. Resilience and responsibility: governing uncertainty in a complex world. *The Geographical Journal* 180 (1): 15-26.

33. Wilbanks, T. J. 2007. Scale and sustainability. *Climate Policy*, 7(4), 278-287. doi:10.1080/14693062.2007.9685656.

34. Wilson, G. A. 2008. From 'weak' to 'strong' multifunctionality: Conceptualizing farm-level multifunctional transitional pathways. *Journal of rural studies*, *24*(3), 367-383.

35. Wilson, G. A. 2013. Community resilience, social memory and the post-2010 Christchurch (New Zealand) earthquakes. *Area*, *45*(2), 207-215.

36. Wilson, G. A. 2013. Community resilience, social memory and the post-2010 Christchurch (New Zealand) earthquakes. *Area*, *45*(2), 207-215.

37. Wilson, G. A. 2015. Community resilience and social memory. *Environmental Values*, *24* (2), 227-257.

38. Wilson, G. A. 2018. "Constructive tensions" in resilience research: Critical reflections from a human geography perspective. *The Geographical Journal*, 184 (1), 89-99. www.ecologyandsociety.org.

PART THREE: INTERNATIONAL STANDARDS AND STANDARDIZATION + PANDEMICS AND EPIDEMICS

Sonja Cindori*)

Iris Stanković**)

UDC: 343.9.024:336.7]:341.24(4-672EY)
343.9.024:336.7]:340.13(497.5)

CHALLENGES IN TRANSPOSING DIRECTIVE 2018/843 INTO THE CROATIAN LEGISLATIVE FRAMEWORK

***Abstract**: Directive 2018/843 is one of the most valuable documents regarding recent anti-money laundering and terrorist financing measures to directed towards enhancing the Directive 2015/849. While transposing both directives, the Republic of Croatia amended as many as 65 regulations. The most comprehensive and significant amendments are related to the Act on Prevention of Money Laundering and Financing of Terrorism. Some of the substantial novelties of the Directive 2018/843 refer to the expansion of subjects obliged to implement the prescribed measures, changes in the field of due diligence, and new steps for increased data transparency. The amendments aim to increase the European Union's efforts to combat illegal activities by preventing the misuse of the financial system for money laundering and terrorist financing and causing a direct impact on their penalization.*

***Key words**: risk assesment, due diligence, financial crime, beneficial owner, register, virual currency, politically exposed person, COVID-19*

INTRODUCTION

Most commonly, money laundering (hereinafter ML) has an international character, therefore the measures applied on the level of an individual country can produce only a limited effect. Money laundering, as a process, isn't always carried out by the same persons that conduct criminal and illicit activities. Criminals hire professional money launderers due to their knowledge of international capital markets and competence to assess the risk of detecting unlawful activities, as well as acess to information of differences in the implementation of anti-money

*) Faculty of Law of the Unviersity of Zagreb, Republic of Croatia.
**) ERSTE&STEIERMÄRKISCHE BANKA d.d., Republic of Croatia

laundering (hereinafter AML) law in national legislations (Savona 2005, 95). Professional money launderers can participate in all or only one stage of the ML cycle (placement, layering, and integration) and can provide services to manage, collect, or move funds (FATF 2018, 15). Their service is charged depending on the complexity of the scheme, methods used and knowledge of the predicate offence (FATF 2018, 11). Along with individuals, there are also professional ML organizations that act in a more sophisticated manner and can provide the entire infrastructure for complex ML schemes or construct a unique scheme, tailored for the specific needs of a client (FATF 2018, 15). Funds to be laundered are often directed to the purchase of financial instruments and other types of assets such as real estate, especially located in the countries where funds can be utilized without obtaining information on the source of funds (Savona 2005, 94).

Money laundering and terrorist financing (hereinafter ML/TF) preventive measures brought by organizations such as the Financial Action Task Force (hereinafter FATF) and the European Commission are being created with the task of protecting the integrity of the financial sector and combatting the ML/TF. These measures ensure tracing, seizing, freezing, and confiscating criminal assets and criminal prosecution as a repercussion for the criminals. The measures seek to promote the rule of law and are a significant component of an efficient legal system, business-friendly environment and long-term economic and financial development. Following their full and effective implementation, they form an integral part of good financial management, as well as an essential part of the fight against all forms of criminal activities that threaten local, national, and international communities (Asmal 2007, XIX-XX).

In addition to the obligation to apply the measures brought by the European Union (hereinafter EU) by all the Member States, the effect of the EU Directives is also being extended to third countries. Thus, the spatial application field of the Directive 2018/843 on the prevention of the use of the financial system for the

purposes of money laundering or terrorist financing (hereinafter the Fifth Directive) has been extended to Iceland, Norway and Liechtenstein (Stessens 2003, 21) in accordance with the Agreement on the European Economic Area (94/1/EC ECSC 1993).

Along with the first three EU ML/TF directives, the Fifth Directive is a part of the Action Plan against terrorist financing (hereinafter TF), set out by the European Commission in February of 2016. The plan is a reaction to terrorist attacks in Paris in 2015, Brussels in 2016, and Panama Papers leak in 2016. Adoption of the Directive aims to strengthen the combat against TF and increase transparency of financial transactions and structures of corporate and legal entities and other legal arrangements. The Fifth Directive entered into force on July 9, 2018, and the deadline for transposition into the national legislation of the Member States was January 10, 2020. Extent of the changes brought by the Fifth Directive are best explained by the fact that the Republic of Croatia amended as many as 65 regulations while transposing its content. Among the member states with most amended regulations, it is worth to stressing that the Czech Republic made 52 regulations, Hungary 37 and Slovakia 34. Italy (2), Germany, Greece and Portugal (1) are at the end of the list, with the fewest changes in regulations.

Money laundering/terrorism financing represent harmful actions on a global scale, with a devastating impact on many economies. The risk of the ML/TF is the risk of abusing the financial system for illegal purposes by the individual through, i.e., utilization of business relationship, transaction, or product in/directly for ML/TF. At the early stages of combat against ML/TF, the United Nations adopted the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, ratified by Republic of Croatia in 1994 (Government Decision on Ratification 1990/1994), which was followed by many conventions in similar fields, i.e., transnational organized criminal, corruption, etc.

The EU Directives are harmonized with FATF Recommendations, the most important international organization for adopting standards regarding measures, procedures and recommendations for actively promoting and evaluating the system for preventing ML/TF. Some of the recent, quite significant documents, with notable contribution to the field, are the Convention on Cybercrime from 2002 and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism from 2005. Nevertheless, the most significant acts in AML field are the beforementioned Fifth Directive, and its predecessor Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, as well as the amending Directives 2009/138/EC and 2013/36/EU (hereinafter the Fourth directive).

The crucial Croatian act regulating measures for the prevention of the use of the financial system for ML/TF is the Act on Prevention of Money Laundering and Financing of Terrorism (hereinafter the AMLTF Act), which implemented the measures of the Fourth Directive into the Croatian national legislation. Given the Fifth Directive, which partially amends and supplements the Fourth Directive, was adopted in a short period, the Republic of Croatia was obliged to harmonize its legislation with the new international standards. According to mentioned requirements, the new Act on Prevention of Money Laundering and Terrorist financing was adopted and entered into force in 2019.

The response to the recent threats from ML/TF is reflected in the amendments to the previous act. The amendments prompted the adoption of new and more detailed provisions that consist of the following: introduction of public access to data from the Register of Beneficial Owners and introduction of new categories of entities obliged to apply ML/TF measures (legal and natural persons engaged in the activity of providing virtual currency exchange services and fiduciary currencies, as well as the activity of providing wallet custodial services, real estate rental brokers and art dealers).

The concept of virtual currency is defined as well. The new law limits the area of use of prepaid cards and makes the establishment of an appropriate risk management system concerning politically exposed persons mandatory. Given that many legal entities from the EU conduct business with companies and other legal entities from high-risk countries, an obligation of enhanced customer due diligence is introduced when establishing relations and carrying out these kinds of transactions. In addition to the above, the act introduces several additional measures to combat financial crime that contribute to the challenges faced by obliged entities.

1. EXPANSION OF THE SCOPE OF OBLIGED ENTITIES TO IMPLEMENT THE MEASURES DEFINED BY THE FIFTH DIRECTIVE

The obliged entities are applying numerous measures of continuous actions and activities to recognize, assess, understand and reduce the risk of ML/TF. That is reflected in the obligation to carry out due diligence, not only when establishing a business relationship with a client, but continuously during its monitoring, notably in all cases specified in Article 16 of the AMLTF Act. Tasks and procedures carried out by the obliged entities include all necessary actions directed towards ensuring identification of their clients in the processes of risk assessment and monitoring. They help identify and prevent ML/TF and other illegal acts of corruption. According to the United Nations, an average of 2.7% of the global gross domestic product is laundered annually. In relation to the gross domestic product, it is worth noting that it amounts to 1.6 trillion US dollars (United Nations Office on Drugs and Crime 2011, 127). The responsibility for compliance with the AMLTF Act rests with the obliged entities that may be subject to fines in case of non-compliance. According to data presented by Corlytics Ltd., during 2021, a total of 1.6 billion dollars in fines was collected worldwide due to

non-compliance with regulations aimed at preventing ML/TF. According to the Financial Inspectorate, during the same year, in the Republic of Croatia, a total of HRK 202,000 of fines were imposed on legal entities, as well as HRK 23,000 fines on natural persons (Ministry of finance 2022) due to the same reason.

The latest development in technology led to new forms of ML/TF. Modern means of exchange, in particular electronic money and virtual currencies (so-called cryptocurrencies), are accepted as legal means of payment in many countries, given their simplicity and anonymity of use.

The advantages of virtual currency are reflected in the free and rapid transfers around the globe, as well as sustainability, transparency, and inability to block transactions due to economic or political turmoil and the absence of inflation, while their value is based on supply and demand. On the other hand, disadvantages of virtual currencies, such as dealing in good faith, risk of ML, tax evasion, online crime, limited group of users, fluctuations in the value of virtual money, risk of collapse or virtual currency breakdown, and lack of regulation, can be considered as the reasons for lack of acceptance from the general public (Richter, Kraus and Bouncken 2015, 580-582). Virtual currency provides criminals with an easier method of structuring or smurfing, since technology can support splitting up large transactions through standardized and scarcely risky procedures. Accordingly, it is easier to escape controls on financial transactions and minimize the use of human or IT resources devoted to these activities (Stokes 2012, 221-236).

Given that the new kind of payment models were developed after the adoption of the Fourth Directive, this arose a need to expand the scope of the ML/TF provisions. Different kind of entities, such as providers of currency storage and exchange services, were detected by the authors of the Fifth Directive as notable actors in increasing the transparency of such transactions; moreover, they were covered by the Fifth Directive as new obligated entities. In addition to increasing the transparency of transactions and transparency of the ownership structures,

the number of virtual currencies users increases as well. There is, frequently, a complex ownership structure behind a user as a legal person. The main goal of that kind of a structure can be concealing the real owners and currency holders, with the aim of concealing criminal activities.

The transposition of the Fifth Directive into the Croatian legislation can be also found in Art. 9, paragraph 2 of the AMLTF Act, in which the legal and natural persons engaged in the activity of providing virtual and fiduciary currency exchange services and natural persons engaged in the activity of providing wallet custodial services, were added to the scope of the obliged entities. Transposing the Directive's measures and expanding the scope of obliged entities dealt a huge blow to some companies in the EU which offer the mentioned services.

The following extension of the Fifth Directive refers to the activities already covered in terms of obliged entities by the Fourth Directive. In addition to lawyers, notaries, auditors, accountants, and tax advisors, who are listed as obliged entities in Fourth Directive, the Directive added any other person that undertakes to provide, directly or by means of other persons to who that other person is related, material aid, assistance or advice on tax matters as principal business or a professional activity (Directive 2018/843 2018, Article 1).

The last activity is related to the works of art, their purchase, and storage in particular. The ratio of that provision is that works of art are often treated and managed like stocks or real estate or used to invest and generate profit. At a time of extremely low-interest rates, when investment is not profitable in traditional forms of assets or in keeping the money in the bank, a logical decision is imposed to search for new ways of creating capital. For example, in 2017, in the short period, the world's largest auction houses sold works of art worth more than two billion dollars. One of these pieces was Leonardo da Vinci's painting entitled Salvator Mundi, which sold for $450.3 million, making it the most expensive painting ever sold on the art market (Christie's 2017). Although these are legal investments, there is room for ML as well.

2. CHANGES IN THE REGULATION OF EXCEPTIONS TO THE OBLIGATION TO CARRY OUT A CUSTOMER DUE DILIGENCE REGARDING ELECTRONIC MONEY TRANSACTIONS

Although cash represents a fast and efficient method of payment, it has numerous disadvantages. The storage of cash is accompanied by many costs, including costs of the treasury, fraud, loss of money, safekeeping, depositing, as well as costs related to cash management in financial institutions (Hamdi 2007, 289-303). On the other hand, electronic money imposes many advantages. Electronic money means electronically, including magnetically, stored monetary value, as represented by a claim on the issuer which is issued on receipt of funds, directed towards making payment transactions, and which is accepted by a natural or legal person other than the electronic money issuer (Zakon o elektroničkom novcu 2018, Article 3).

Its main role is to support electronic commerce via the Internet, enable fast transactions, reduce costs, and replace payments with banknotes and coins in retail (Hamdi 2007, 289-303). The best example of electronic money is depicted in prepaid cards issued by banks and card companies. Important features of prepaid cards are manifested as having no connection to a bank account, credit limit, and ease of payment. Anonymity and a wide international network of ATMs make it possible to withdraw cash in a country other than the country of the payment (Cheney and Rhine 2006, 2).

In addition to their usability, the advantages of prepaid cards facilitate ML activities, TF, and related logistics. It is more convenient to transfer a prepaid card across the border to another country than to manipulate with cash. Furthermore, it can be sent by post. When the card arrives in the destination country, it can be

used to withdraw funds at numerous ATMs and for TF purposes. The behavior of prepaid card users that can be considered as indicators of illegal actions is depicted in the following: large amounts of cash deposits to the card, inexplicable transactions beyond the usual activities and behavior of the card owner, the simultaneous purchase of a large number of cards by a smaller denomination with the intention of avoiding the obligation to undertake due diligence measures when purchasing an individual card of a higher denomination, etc. (Choo 2008, 3-4).

3. CHANGES IN THE APPLIANCE OF CUSTOMER DUE DILIGENCE MEASURES

Customer due diligence measure is a cornerstone of the AML system. The measure is commonly connected to the "know your customer" (KYC) procedure, which implies taking all measures of identification (the identity of the natural person and the identity of the beneficial owner of the legal entity) and data collection on the nature and purpose of a business relationship, wherefore it is possible to assess the risk of ML/TF associated with that particular client (FATF 2022, 14).

The latest technical developments are enabling the performance of secure remote or electronic identification that can replace the traditional identification process. Digitization of society on a global level is ubiquitous, given the growing need for the establishment of secure electronic identification and authentication. The establishment of a secure electronic identification system is an elementary condition for further successful development of the digital economy and a cornerstone for progress towards a single digital market (Deloitte 2018, 5). The same trend is followed in the AMLTF Act, which allows any secure, remote, or electronic identification procedure regulated, recognized, approved, or accepted by the relevant national authorities. It opens the possibility of using a qualified

certificate for an electronic signature and an electronic seal to determine and verify the client's identity, as well as video-electronic identification (Pravilnik o minimalnim tehničkim uvjetima koje moraju ispunjavati sredstva videoelektroničke identifikacije 2019, Article 1).

The future of electronic identification is, undoubtedly, the application of biometrics. Currently, security systems based on biometric recognition characteristics are usually used to control access to particular systems after the client's previous identification by standard methods. In this regard, the client is identified by a biometric method of identification (e.g., fingerprint, facial appearance, iris, and retina of the eye) and consequently enables access following previously determined powers and duties (Radmilović 2008, 159-180).

4. POLITICALLY EXPOSED PERSONS

The customer due diligence measures are not carried out in relation to all clients and transactions. When implemented, they are intended for certain situations, implemented in order to conduct a simplified, and for other particular cases to conduct enhanced customer due diligence measures. In terms of politically exposed persons (hereinafter PEP), an enhanced customer due diligence is applied.

Due to their position and influence, many PEPs can potentially be forced to commit ML and related predicate offenses, including corruption and bribery, as well as conducting activities related to the TF. Therefore, the Fifth Directive and FATF Recommendations require countries to ensure the conditions under which financial institutions, certain non-financial companies, and other professions, implement measures to prevent the abuse of the financial system and non-financial companies and professions by PEPs, i.e., detection of such potential abuse if and when it occurs (FATF 2022, 3). Such regulation is particularly significant given the current sanctions against Russia concerning the war in Ukraine.

The mere determination that a certain person belongs to the category of PEPs is not the ultimate goal, but rather a part of the process that enables those liable for the implementation of due diligence measures to assess various types of major risks associated with doing business with PEPs. The fact that the client is a PEP does not represent the end of the process of the enhanced customer due diligence, nor does it release the obligated entities from further continuous due diligence measures. Equally, this fact does not prejudge the connection of PEP with criminal activities, nor is it equated with crime or abuse of the financial system. In the same manner, it does not mean that the person in a specific case automatically represents a greater risk; however, it is certainly a signal to obligated entities that an increased attention is needed when doing business and transactions (FATF 2022, 27).

5. ENHANCED CUSTOMER DUE DILIGENCE MEASURES IN BUSINESS RELATIONSHIPS OR TRANSACTIONS INVOLVING HIGH-RISK THIRD COUNTRIES

The European Commission should identify countries with strategic deficiencies in the regime regarding ML prevention and the fight against TF, which represent a significant threat to the financial system of the EU, according to the Fifth Directive. Such countries are marked as high-risk, due to significant weaknesses in their AML/TF regime, which could affect the success of the fight against such illegal actions. The Commission determines high-risk countries by adopting the Delegated Regulations. The first one was adopted in 2016. The Commission Delegated Regulation (EU) 2021/37 on amending Delegated Regulation (EU) 2016/1675 supplementing Directive (EU) 2015/849 is currently in force, as regards deleting Mongolia from the table in point I of the Annex.

The previous Delegated Regulations had to be revised relating to the progress that identified high-risk third countries achieved in eliminating strategic deficiencies in their legislation and practices. When adopting new regulations, the European Commission considers all recent information from international organizations and experts, such as those published by the FATF. The Commission is guided by the idea that every third country, determined by FATF, that poses a risk to the international financial system, poses a risk to the financial system of the EU and its members as well (Commission Delegated Regulation 2020/855 2020, Preamble).

As a result, the following are currently considered as high-risk third countries: Afghanistan, Albania, Bahamas, Barbados, Botswana, DPR Korea, Ghana, Iraq, Iran, Jamaica, Yemen, Cambodia, Mauritius, Myanmar, Nicaragua, Pakistan, Panama, Syria, Trinidad and Tobago, Uganda, Vanuatu, Zimbabwe. The list is made up of the FATF's "blacklist" of countries that pose a high risk (Iran and DPR Korea are currently identified as such) and a "grey list" of countries that are under increased monitoring and are actively cooperating with the FATF to correct deficiencies in their own AML/TF systems. Other countries under increased monitoring are actively working with the FATF to address the strategic deficiencies in their systems in order to counter ML/TF and proliferation financing. When FATF places jurisdiction under increased monitoring, it means that the country has committed to resolving the identified deficiencies in their AML/TF systems within agreed timeframes and is subject to increased monitoring. The FATF constantly identifies additional countries. Since the start of the *Covid-19* pandemic, the FATF has provided some flexibility to countries not facing immediate deadlines to report progress voluntarily.

According to the FATF Recommendations, concerning clients from countries on the "grey list", it is not necessary to apply enhanced customer due diligence, since the client comes from these countries, although the stated circumstance may

be a significant factor for risk assessment. However, the European Commission has designated certain countries on the "grey list" as high-risk third countries; therefore, it is still necessary to apply the enhanced due diligence measures to clients from these countries. Furthermore, the European Commission has designated certain countries not covered by the FATF Recommendations as high-risk states, such as Afghanistan, Iraq, Trinidad, Tobago, and Vanuatu (Ministry of finance 2022, 3).

6. COVID-19 CHALLENGES

At the time of the *Covid-19* pandemic, the focus of interest was entirely directed towards suppressing a new and dangerous disease, while the fight against ML/TF was of secondary importance. Due to the pandemic, a rise in financial crime emphasizing *COVID*-specific crime patterns occurred, such as the counterfeiting of medical goods and scams to exploit economic stimulus measures. Criminals use the opportunities created by the pandemic across the world, with mounting cases of the counterfeiting of medical goods, investment fraud, cyber-crime scams, and exploitation of economic stimulus measures put in place by certain governments (FATF 2020, 6).

There have also been examples of online child exploitation due to an increase in the time spent online, increases in property crime due to properties being left uninhabited, and corruption related to contracts for medical supplies. Criminals used an increase in online activity to develop targeted malware campaigns, ransomware, or phishing attacks containing fake links to government stimulus packages and websites selling personal protection supplies. The pandemic, unfortunately, correspondingly resulted in an increase in human trafficking, exploitation of workers, and most disturbing of all, with children spending more time online, more online child exploitation has been recorded. The pandemic has

left many businesses or individuals needing financial aid. Criminals used them as easy targets to take part in ML activity, i.e., by using a failing, although legitimate business as a front for illicit activity. The economic volatility has resulted in several other ML vulnerabilities, such as an increase in unregulated financial services and insider trading from the large shifts in value due to the pandemic. There have also been cases of virtual assets misuse in *Covid-19*-related fraud, including money mule scams that target the recently unemployed or furloughed (Lewis 2021).

Due to the evolving impacts of the pandemic, the changes in ML/TF activity caused by the pandemic are likely to continue to develop as well. Rising unemployment, financial distress, bankruptcy of companies, increased circulation of cash in economies, potential stockpiling of cash by organized criminal groups, and the accelerated implementation of stimulus programs, represent vulnerabilities that criminals may exploit over the coming period. Furthermore, as the development of new *Covid-19* vaccines accelerates, so too will opportunities for criminals to devise criminal scams to exploit and illegally profit from these new medical advancements. While there are some globally consistent trends, other risks may be specific to particular countries or regions (FATF 2020, 21).

7. INFORMATION TRANSPARENCY MEASURES

Legal entities and other legal arrangements, such as trusts, foundations, and many others (hereinafter legal entities) participate in a wide range of commercial and entrepreneurial activities that can be misused for illegal purposes. The abuse of legal entities could be significantly reduced if information about the legal owner (the owner of shares, shares, etc.) and the beneficial owner (the one who controls the entity) were available to the authorities and the public. The information about the legal owner of the entity is listed in the official registers of the state under

whose jurisdiction the entity operates, while this is not the case for information about the beneficial owners.

Beneficial owner identification for an individual legal entity can serve the authorities during investigations and gathering information about the money flow when observing suspicious actions and transactions (FATF 2014, 3). The issue of using legal entities for criminal purposes is increased by numerous legal forms of entities in different jurisdictions and their different tax and legal treatment. The main goal is to conceal information about the beneficial owner. Some recognized forms of abuse are the establishment of fictitious companies (so-called shell companies), the establishment of entities with complex ownership structures that include many layers of ownership with different owners, the use of trusts, and other legal arrangements that enable the separation of legal ownership and beneficial ownership of property, the use of intermediaries in the establishment of legal entities, etc.

Criminals often create, control, and finance legal entities from different countries, thereby disabling access to relevant information. In addition, they establish numerous legal entities that are *de facto* related persons, although they appear to be independent entities, between which they carry out legal transactions. In principle, these are fictitious legal transactions that serve to launder money. Due to the lack and delay of information about the beneficial owner of these entities, it is impossible to follow the money trail, which ultimately prevents timely investigation and reaction (FATF 2014, 6-7).

Before the adoption of the Fifth Directive, all legal entities established on the territory of the Member States had the obligation to obtain and keep correct and up-to-date information about their beneficial owners. The Fifth Directive brings novelty regarding the responsability of Member States to provide the public access to information on the beneficial ownership of legal entities through central registers. The AMLTF Act regulated the establishment, organization, and

management of the Registry of Beneficial Owners (hereinafter Registry) as a central electronic database on the beneficial owners of companies, branches of foreign companies, associations, foundations, institutions, trusts, and trust-equivalent entities under foreign law. The Registry is established, maintained, and managed by the Financial Agency (hereinafter FINA) on behalf of the Ministry of Finance, the Anti-Money Laundering Office. FINA is in control of collecting, recording, processing, updating, and archiving data from the Registry (Zakon o sprječavanju pranja novca i financiranja terorizma 2019, Article 32). According to the AMLTF Act, the Ordinance on the Register of Beneficial Owners was adopted.

8. ESTABLISHING CENTRALIZED AUTOMATED MECHANISMS FOR ACCESS TO INFORMATION ON THE IDENTITY OF HOLDERS, PROXY HOLDERS, AND BENEFICIAL OWNERS OF BANK AND PAYMENT ACCOUNTS AND SAFE-DEPOSIT BOXES

The centralized automated mechanism for access to information on the identity of holders, proxy holders, and beneficial owners of bank and payment accounts and safe-deposit boxes was established in the Republic of Croatia in 2002 under the name “The Unified Account Registry” (hereinafter JRR). The JRR is an electronic database that contains records of all regular accounts held by business entities, budget accounts, and accounts for the collection of joint budget revenues held with banks in Croatia and the Croatian National Bank. It is mantained by FINA, and contains records of all bank deposit accounts.

The deadline for the establishment of the centralized automated mechanism for access to information on the identity of holders, proxy holders, and beneficial owners of bank and payment accounts, as well as safe-deposit boxes, has been set

by Fifth Directive to be October 10th, 2020. The transposition was carried out by amending the Act on Execution of Enforcement over Monetary Assets, by which, in addition to data on owners and account numbers, information on safe-deposit boxes of natural and legal persons must be submitted to the JRR. New information, that shall be accessible and searchable through the JRR, is the information on the beneficial owner of the account holder, as well as information about any person purporting to act on behalf of the customer. Furthermore, the Fifth Directive ordered the Member States to prohibit their credit and financial institutions from keeping anonymous accounts, passbooks, or safe-deposit boxes. For current anonymous accounts, passbooks, or safe-deposit boxes, customer due diligence measures shall be performed before their use.

In order to respect privacy and protect personal data, the Fifth Directive requires minimum data necessary for carrying out ML/TF investigations, that should be collected and held in centralized automated mechanisms. The Member States can determine the exact data that must be gathered, considering the systems and legal traditions in place to enable identification of the beneficial owners. The Member States should determine the period for retention of the information collected within the application of customer due diligence measures as well. With the aim to transpose all those provisions, the Croatian legislators introduced the Ordinance on the Unified Account Registry. The establishment of centralized automated mechanisms for each member State should result in timely access to information on the identity of holders of bank and payment accounts and safe-deposit boxes, their proxy holders, and their beneficial owners to its national Financial Intelligence Unit. Proper access to information is necessary in order to effectively mitigate the risks associated with ML/TF.

CONCLUSION

Money laundering/terrorism funding takes its place in the financial market and other exposed areas on an international scale, but also in numerous countries. Considering the possibility of free movement of capital and accessibility of financial services misusage, the EU adopted several directives to protect the integrity, inviolability, and stability of financial institutions and trust in the financial system. The first two directives were founded on a rule-based approach, while the Third Directive regulated the prevention of TF in addition to the area of ML prevention, along with the introduction of a risk-based approach. The Fourth and Fifth Directives rest on the same foundations and elaborate risk assessment systems comprehensively and are directed towards identification, assess, understanding, and reducing the risks. What stands out, in particular, are the standards manifesting an undeniable connection between terrorism and transnational organized crime. Those create the basis for preventing terrorist groups from gaining access to international financial institutions by expanding the framework for more severe sanctions.

All the changes brought by the Fourth Directive and the Fifth Directive represent the expansion of the scope of the Third Directive and the adoption of an increasing number of targeted measures. The most important provisions that have been implemented in the national legislation are aimed towards establishing an effective and comprehensive legal framework for overcoming the problems of ML/TF. By extending the scope of the provisions to new obligated entities, the authorities of the Member States gained widened insight into business relationships and transactions that were previously anonymous. Information about relationships and transactions are being collected and examined with the aim of establishing links between suspicious transactions and related criminal activity.

The enhanced due diligence measures, new data gathering, and customer identification methods, as well as public access to particular information, facilitate the timely and efficient availability of information to the national and third country Financial Intelligence Units and authorities. A high degree of transparency and processing of illegal activities affects the trust of the public, investors, and other actors in the financial market, which is necessary for the growth and further development of the economy. By far, the most significant factors for attracting foreign investors are the transparency and security of a business. The Republic of Croatia considers it very important since the national economy depends on foreign investments and capital outside the borders.

REFERENCES

1. Asmal, Kader. 2007. Foreword. *Anti-Money Laundering: International Law and Practice by Muller, Wouter H., Christian H. Kälin, and John G. Goldsworth.,* Chichester: John Wiley & Sons.
2. Cheney, Julia S. & Sherrie L. W. Rhine. 2006. *Prepaid cards: an important innovation in financial services,* Philadelphia: Federal Reserve Bank of Philadelphia.
3. Choo, Kim-Kwang Raymond. 2008. *Money laundering risks of prepaid stored value cards. Trends & issues in crime and criminal justice*, Canberra: Australian Institute of Criminology.
4. Christie's. 2017. "Leonardo's Salvator Mundi makes auction history". https://www.christies.com.
5. Deloitte. 2018. *Looking ahead: The user experience of eIDAS-based eID*, European Commission. https://ec.europa.eu.
6. FATF. 2012-2022. *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, FATF, Paris, France. https://www.fatf-gafi.org.
7. FATF. 2013. *FATF Guidance Politically Exposed Persons (Recommendations 12 and 22)*, FATF/OECD, Paris, France. https://www.fatf-gafi.org.
8. FATF. 2014. *FATF Guidance Transparency and beneficial ownership*, FATF/OECD, Paris, France. https://www.fatf-gafi.org.
9. FATF. 2018. *Professional Money Laundering*, FATF, Paris, France. https://www.fatf-gafi.org.
10. FATF. 2020. *Update: COVID-19-related Money Laundering and Terrorist Financing, COVID-19-related Money Laundering and Terrorist Financing – Risks and Policy Responses*, FATF, Paris, France. https://www.fatf-gafi.org.
11. Hamdi, Helmi. 2007. *Problemi razvoja elektroničkog novca*, Financijska teorija i praksa 31 no. 3.

12. Lewis, David. 2021. *Covid-19 and the Changing Money Laundering and Terrorist Financing Risk Landscape.* Remarks at the MENA Regtech Virtual Executive Boardroom, 18 January 2021. https://www.fatf-gafi.org.

13. Ministry of Finance, Financial Inspectorate. 2022. *Lista visokorizičnih trećih država sa strateškim nedostacima u sustavima sprječavanja pranja novca i financiranja terorizma*. https://mfin.gov.hr.

14. Ministry of Finance, Financial Inspectorate. 2022. *Objava podataka o prekršajnim sankcijama iz područja SPNFT*. https://mfin.gov.hr.

15. Official Gazette. 1994. *Odluka vlade o ratifikaciji Konvencije Ujedinjenih naroda protiv nezakonitog prometa opojnih droga i psihotropnih supstanci iz Odluke o objavljivanju mnogostranih međunarodnih ugovora kojih je RH stranka na temelju notifikacija o sukcesiji*. Zagreb: Narodne novine d.d. (Međunarodni dio br. 4/94) Originalni tekst objavljen u Službenom listu SFRJ, Međunarodni ugovori, broj 14/90.

16. Official Gazette. 2002. *Zakon o potvrđivanju konvencije o kibernetičkom kriminalu*. Zagreb: Narodne novine d.d. (no. 9/2002).

17. Official Gazette. 2008. *Zakon o potvrđivanju konvencije Vijeća Europe o pranju, traganju, privremenom Narodne novine oduzimanju i oduzimanju prihoda stečenoga kaznenim djelom i o financiranju terorizma.* Zagreb: Narodne novine d.d. (no. 5/2008).

18. Official Gazette. 2012. *Zakon o zaštiti osobnih podataka.* Zagreb: Narodne novine d.d. (no. 103/03, 118/06, 41/08, 130/11, 106/12).

19. Official Gazette. 2018. *Zakon o elektroničkom novcu*. Zagreb: Narodne novine d.d. (no. 64/18).

20. Official Gazette. 2019. *Pravilnik o minimalnim tehničkim uvjetima koje moraju ispunjavati sredstva videoelektroničke identifikacije*. Zagreb: Narodne novine d.d. (no. 1/19).

21. Official Gazette. 2019. *Zakon o izmjenama i dopunama Zakona o sprječavanju pranja novca i financiranju terorizma.* Zagreb: Narodne novine d.d. (no. 39/19).

22. Official Gazette. 2019. *Zakon o sprječavanju pranja novca i financiranja terorizma.* Zagreb: Narodne novine d.d. (no. 108/2017, 39/2019).

23. Official Gazette. 2020. *Pravilnik o jedinstvenom registru računa*. Zagreb: Narodne novine d.d. (no. 53/2020).

24. Official Gazette. 2020. *Pravilnik o Registru stvarnih vlasnika*. Zagreb: Narodne novine d.d. (no. 23/2019, 1/2020).

25. Official Gazette. 2020. *Zakon o provedbi ovrhe na novčanim sredstvima.* Zagreb: Narodne novine d.d. (no. 68/18, 02/20, 46/20, 47/20).

26. Official Journal of the European Union. 1994. *94/1/EC, ECSC: Decision of the Council and the Commission of 13 December 1993 on the conclusion of the Agreement on the European Economic Area between the European Communities, their Member States and the Republic of Austria, the Republic of Finland, the Republic of Iceland, the Principality of Liechtenstein, the Kingdom of Norway, the Kingdom of Sweden and the Swiss Confederation*. Luxembourg: Publications Office of the European Union (no. L 1, 3.1.1994).

27. Official Journal of the European Union. 2015. *Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC*. Luxembourg: Publications Office of the European Union (no. L 141/73, 5.6.2015).

28. Official Journal of the European Union. 2018. *Direktiva (EU) 2018/843 Europskog parlamenta i Vijeća od 30. svibnja 2018. o izmjeni Direktive (EU) 2015/849 o sprečavanju korištenja financijskog sustava u svrhu pranja novca ili financiranja terorizma i o izmjeni direktiva 2009/138/EZ i 2013/36/EU* Luxembourg: Publications Office of the European Union (no. L 156, 19.6.2018, p. 43-74).

29. Official Journal of the European Union. 2020. *Commission Delegated Regulation (EU) 2020/855 of 7 May 2020 amending Delegated Regulation (EU) 2016/1675 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council, as regards adding the Bahamas, Barbados, Botswana, Cambodia, Ghana, Jamaica, Mauritius, Mongolia, Myanmar/Burma, Nicaragua, Panama and Zimbabwe to the table in point I of the Annex and*

deleting Bosnia-Herzegovina, Ethiopia, Guyana, Lao People's Democratic Republic, Sri Lanka and Tunisia from this table. Luxembourg: Publications Office of the European Union (no. L 195, 19.6.2020, 1–8).

30. Official Journal of the European Union. 2021. *Commission Delegated Regulation (EU) 2021/37 of 7 December 2020 on amending Delegated Regulation (EU) 2016/1675 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council, as regards deleting Mongolia from the table in point I of the Annex C/2020/8386.* Luxembourg: Publications Office of the European Union, (no. L 14, 18.1.2021, 1–3).
31. Radmilović, Želimir. 2008. *Biometrijska identifikacija.* Policija i sigurnost, 17 (3-4).
32. Richter, Chris, Sascha Kraus, and Ricarda B. Bouncken. 2015. *Virtual Currencies like Bitcoin as a Paradigm Shift in the Field of Transactions*. International Business & Economics Research Journal 14 no. 4 (July/August): https://doi.org.
33. Savona, Ernesto Ugo. 2005. *Responding to Money Laundering International Perspectives*. Amsterdam: Harwood Academic Publishers. Taylor & Francis e-Library.
34. Stessens, Guy. 2003. *Money Laundering, A New International Law Enforcement Model*. Cambridge: Cambridge University Press. NetLibrary.
35. Stokes, R. 2012. *Virtual money laundering: the case of Bitcoin and the Linden dollar*. Information and Communications Technology Law 21 no. 3, https://doi.org.
36. United Nations Office on Drugs and Crime. 2011. *Research report: Estimating illicit financial flows resulting from drug trafficking and other translational organized crimes.* https://www.unodc.org.

Jelena Slović*)

UDC: 623.45:005.334
623.45:657-051
623.45:657.6-051

IDENTIFICATION OF PROLIFERATION FROM THE PERSPECTIVE OF PROFESSIONAL ACCOUNTANTS AND AUDITORS

Abstract: *The proliferation of weapons of mass destruction is an area that is still not sufficiently known, nevertheless it has gained great importance in the current international situation because it poses a direct or indirect threat to human lives, as well as to the entire financial system and economy. Considering that professional accountants and auditors, among the others, appear in the capacity of Designated Non-financial Business and Professions, this paper researches the role and contribution of these professions in identifying the proliferation of weapons of mass destruction. The first step to get the result is establishing a proper definition for the proliferation of weapons of mass destruction and, accordingly, determine the function of professional accountants and auditors in the process of proliferation identification.*

Key words: *Proliferation, Professional Accountants and Auditors, Public Private Partnership, Weapons for Mass Destruction.*

INTRODUCTION

The importance of prevention in the area of proliferation is recognized and regulated by resolutions of United Nations Security Council (hereinafter: the UN SC), as the recommendations given by the Financial Action Task Force (hereinafter: the FATF). Resolution 1540, adopted in 2004, should be specially highlighted here, given that in this resolution the UN SC calls upon all states to promote dialogue and cooperation on nonproliferation so as to address the threat posed by proliferation of nuclear, chemical, or biological weapons, and their means of delivery, as well as to take cooperative action to prevent illicit trafficking in nuclear, chemical or biological weapons, their means of delivery, and related materials (UN SC, 2004, 4).

*) Auditing Company ECOVIS FinAudit, Ljubana Jednaka 1, Belgrade, Serbia, jelena.slovic@ecovis.rs.

Also, the European Council (hereinafter: the EC) identified in its European Security Strategy (hereinafter: the ESS) a range of threats and challenges to the European Union (hereinafter: the EU) security interests, in which the proliferation of weapons for mass destruction (hereinafter: proliferation) is classified as potentially the greatest threat to the EU security (EU Council, 2009, 12). The EC in 2003 adopted the European strategy against the proliferation of weapons of mass destruction, and in order to mitigate proliferation risk, it launched chemical, biological, radiological and nuclear Centres of Excellence initiative in 2010. This initiative is designed to strengthen the institutional capacity of the non-EU countries to mitigate chemical, biological, radiological and nuclear risks which, if not countered, may constitute a threat to the EU (European Court of Auditors, 2014, 7).

The FATF applied the following broad working definition of proliferation and proliferation financing: "Proliferation is the transfer and export of nuclear, chemical or biological weapons; their means of delivery and related materials. This could include, *inter alia*, technology, goods, software, services or expertise" (FATF, 2008, 2). Proliferation financing refers to: the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations (FATF/OECD, 2010, 11). Recommendation 7 of the FATF Recommendations requires countries to implement Targeted Financial Sanctions in order to comply with the UN SC resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing (FATF, 2022, 13). Recommendation 2 requires countries to put in place effective national cooperation and, where appropriate, coordination mechanisms to combat the financing of proliferation (FATF, 2022, 11).

1. BASICS OF THE PROLIFERATION FINANCING CONCEPT

In the context of this work, the term of proliferation financing, as defined by the FATF, is relevant for further considerations, and as such, it should be emphasized: *Proliferation financing* is providing financial services for the transfer and export of nuclear, chemical or biological weapons; their means of delivery and related materials. It involves, in particular, financing of trade in proliferation of sensitive goods, but could also include other financial support to individuals or entities engaged in proliferation (FATD/OECD, 2010, 11).

In the context of FATF Recommendation 1, countries should also identify, assess, and understand the proliferation financing risks for the country. In order to mitigate proliferation risks, countries should develop an understanding of the means of potential breaches, evasion and non-implementation of targeted financial sanctions present in their countries that can be shared within and across competent authorities and with the private sector (FATF, 2022, 11). Countries should ensure that financial institutions and DNFBPs take steps to identify circumstances, which may present higher risks and ensure that their Counter Proliferation (CPF) regime addresses these risks (FATF, 2022, 34).

Since proliferation has more in common with terrorist financing than money laundering (Bilandzic in Cindori's, 2017, 99), then countries, in order to fight against money laundering, terrorist financing and proliferation, should require financial institutions and DNFBPs to identify, assess and take effective action to mitigate their money laundering, terrorist financing and proliferation financing risks (FATF, 2021, 10). Also, FATF defines that professional accountants in public practice and auditors in capacity of DNFBPs may provide a wide range of services to a diverse range of clients (FATF, 2019, 12).

2. MULTIDISCIPLINARY ACCESS

Activities in the sphere of finance related to the detection of proliferation are mainly focused on the monitoring of banking transactions and cash flows, which is expedient, but not sufficient. The EU in its ESS identified the complexity of proliferation. In order to combat it, it is necessary to apply a mixture of instruments. An essential part of limiting and preventing proliferation are export controls, as well as the existence of political, economic and other pressures, while the underlying political causes are also tackled (Council of the EU, 2009, 35). Coordinated synergistic activities of DNFBPs from various fields, including accountants and auditors, can contribute and direct towards finding new or better ways to use expert's knowledge in order to form and recognize suspicion of proliferation of weapons of mass destruction.

Proliferation is a complex phenomenon and includes highly developed scientific and technological knowledge from various scientific disciplines, so it is difficult to identify it in a timely manner. However, what entities in all areas have in common, regardless of whether they are in the private or public and state sectors, is the fact that the work of all experts leaves a certain documentary trail in finance, which is wider and deeper than the cash flows competent authorities usually follow.

The above-mentioned facts impose the need to apply a multidisciplinary access that, in addition to scientists and experts from various scientific, research or security fields, will also include persons who, with their knowledge and understanding of financial aspects of certain transactions, can indicate the existence of suspicion of proliferation.

FATF reports that the ability of a financial institution to identify proliferation risk is limited due to the impossibility of reviewing the complete transactions and implementing risk assessment measures (FATF/OECD, 2010, 42). Limiting factors

relate to the technical expertise available to banks, the availability of limited information as a basis for monitoring accounts and the inability of financial institutions to check their accuracy, the structural difference between money laundering and proliferation financing, as well as the lack of a clear financial model, unique to financing proliferation and fragmentation as a feature of the sales cycle. Based on the above, it can be concluded that the scope and content of the concept of money laundering, terrorist financing and proliferation require appropriate prevention measures (Cindori, 2017, 100).

2.1. BUSINESS IN THE FUNCTION OF PROLIFERATION

As previously defined, proliferation refers to the production, purchase, possession, development, export, trans-shipment, brokering, transport, transfer, storage or use of nuclear, chemical and biological weapons and materials related to them, as well as technology, dual-purpose goods, software, including those services and expertise related to the foregoing (FATF, 2008, 2). If we take into account that effective proliferation includes a large number of activities that demand and take place in certain conditions and a specific environment, then it can be said that business and the various activities it includes provide good conditions for implementation of proliferation.

Business operations include a large number of activities that provide opportunities for carrying out actions necessary for proliferation. These activities, among others, include: procurement of various products and services, transport (by all forms of transportation), forwarding, possession and use of various production, technical, technological, expert, research capacities, as well as import and export. Since all the aforementioned activities can be carried out through business without interruption, this indicates that it enables the smooth flow of materials, products, goods, knowledge and information through regular business activities.

This means that certain aspects of the economic potential of a country simultaneously represent the potential for proliferation of weapons of mass destruction, that can be implemented both within the economy, financial and non-financial sectors, and also within the public and state sectors. Having in mind the steps required to finance and implement proliferation, including sectors other than the financial ones or non-monetary activities, we believe that these circumstances demand that we reconsider the completeness of the FATF definition of financing proliferation. Namely, proliferation can be financed through the financial sector, but it can also be financed by delivery and exchange of different goods or materials and by providing services for their conversion into the desired product, which can be different forms of weapons for mass destruction, and all that can be done without any cash flow or financing in a conservative monetary way. These facts suggest that FATF definition needs to be expanded and that it should be supplemented by adding the non-financial sector as an additional way of financing proliferation besides financial services.

Given that this paper is focused on exploring the potential of professional accountants and auditors in identifying proliferation, further considerations will be focused on the ability of these professionals to use their professional knowledge to identify suspected proliferation in the private, public and government sectors.

2.2. THE SIGNIFICANCE OF A NON-MONETARY ACCESS IN THE IDENTIFICATION OF PROLIFERATION

In the process of identification of proliferation, attention is focused primarily on bank and non-bank transfers and monitoring of cash flows, which has its advantages, but also limitations, given that banks and the financial sector are put in the foreground, while the potential of other DNFBPs, in terms of identifying suspected proliferation, is neglected. The essential idea of this paper is to point out that, in addition to monitoring transfers through the banking and non-banking

sectors, significant information can be obtained from other financial and non-financial data that may indicate proliferation, which are available to different DNFBPs. The financing of proliferation does not have to be done only in a monetary way (cash and cash equivalents), but can be done through the exchange or delivery of certain goods and services, which does not have to leave a cash or monetary trail, because they are realized and settled in other ways, and thus create different documentation trails that can be identified by accountants and auditors.

The advantage of "non-monetary access" for the purpose of proliferation is that there is no need for traces of cash flows, i.e. monetary transfers between participants, whether they are private, public or state companies. It is quite possible that all the processes required for proliferation take place without cash flows, where transfers of goods and services can be settled in other ways (compensations, cessions, assignments) or other forms of settlement that can be used in underdeveloped financial systems (i. e. bilateral barter contracts).

Having in mind the previous consideration, we find that proliferation financing should be redefined and supplemented with additional identifiers in order to include the uncovered area of non-monetary transactions, and it should be done in a following manner: Proliferation financing refers to providing financial support, either in monetary or non-monetary manner for the transfer, conversion, export and use of nuclear, chemical or biological weapons, their means of delivery and related materials. The purpose of redefining proliferation financing is to provide comprehensive definition of this occurrence by including non-monetary transactions, as a common part of this process, and also it could enable DNFBPs to better comprehending of this occurrence and improve identification of suspicious transactions.

Also, this very fact indicates existence of an area that is insufficiently researched, and that is non-monetary transactions for the purpose of proliferation financing. If we accept the above-mentioned wider definition of proliferation

financing that identifies both monetary and non-monetary transactions, than the role of professional accountants and auditors in the identification of proliferation is defined. Concretely, if we accept that proliferation financing includes monetary and non-monetary transactions, then professional accountants and auditors, with their specific expertise, can provide significant contribution in the area of identification of suspicious non-monetary transaction for the purpose of proliferation financing.

2.3. PROFESSIONAL ACCOUNTANTS AND AUDITORS IN THE IDENTIFICATION OF PROLIFERATION

The risk of proliferation is one of the biggest risks that an entity can be exposed to, but it is still not sufficiently recognized and consequently not properly identified by DNFBPs, and thus adequate responses to this risk have not yet been designed. Considering potential of the professional accountants and auditors in the capacity of DNFBPs, we have to bear in mind that these professions are present in both the private and public sectors, which represents their advantage for identifying suspicions of proliferation in both sectors.

Professional accountants and auditors need to gain a sufficient understanding of business activities and processes in the entity, and thus they can very easily notice unusual changes and transactions that may be indicative of proliferation. Also, these professionals have access to financial and non-financial information, and with their specialist's knowledge, they can properly understand and interpret it, including monetary and non-monetary transactions, thus potentially identifying indications of proliferation. This very fact, along with a good understanding of the business processes that takes place in the entity and the understanding of proliferation as an occurrence, gives accountants a great advantage in identifying suspicions about it in a timely manner.

The accounting profession is present in all business segments, because every entity must keep accounting records, and this allows these professions to gain insight into all business transactions that take place, including having access to all documents and records in the entity. However, what can be a limiting factor is that accountants often do not have sufficient knowledge and understanding of the entire business and certain processes in the entity, so they can hardly notice unusual deviations or transactions that may be indicative of suspected proliferation. In addition, if the management or leadership of the entity participates in fraudulent activities, money laundering or proliferation, then it intends to conceal certain information or present it in a certain way in order to mislead. In such a case, the management and leadership are in a position to conduct fraudulent activities and influence the cover-up, including how accountants will present them in financial statements. In this way, accountants can, due to the lack of independence and objectivity in relation to the entity, become complicit in concealment of fraud, money laundering or proliferation.

In addition to audit knowledge, external auditors also possess accounting knowledge, and their advantage is that they possess a sufficient degree of independence and objectivity in relation to the entity. Having professional competence and independence is a great advantage, but also a responsibility of the external audit regarding the potential to identify transactions that are deemed as suspicious for proliferation. With a preliminary good adequate assessment of the audit risk and the risk of money laundering, terrorist financing and proliferation, auditors can use their professional competence to identify unusual transactions that can be potentially suspicious for proliferation. The existence of such deviations indicate that it is necessary to acquire additional knowledge and perform additional tests in order to be able to assess whether they indicate the existence of hidden goals, including proliferation.

When it comes to auditing, it should be borne in mind that, in addition to external auditing, there is also internal auditing, which is not part of professional accountants. However, in terms of the possibility of identifying proliferation,

internal audit has needed specialist knowledge and experience, as well as a good knowledge of the entity that is the subject of the audit, to be able to identify suspicious transactions, so there is a certain potential in this profession as well.

3. RISK OF PROLIFERATION IN THE PUBLIC AND STATE SECTOR

Due to its complexity and comprehensiveness, the state and public sector combines many activities that can be risky, thus making this sector vulnerable. Therefore, when considering the sectoral risk of proliferation, the state and the public sector can be considered as sectors that carry a particularly high risk for proliferation, primarily due to their importance, size and the type of projects carried out in these sectors, as well as the fact that financing is done from the national funds or the EU funds.

As a rule, investments and works in the public and state sector are carried out according to a certain procedure and there should be a certain control. However, no matter how well designed the system is, it does not mean that it works well. The data published by Transparency International in its research on corruption in EU countries shows that the majority of EU citizens believe that corruption exists in both the public and private sectors, while it especially points out the corruption of government bodies, but also of the private sector, as well as that there are close ties between business and politics, whilst the business uses bribes or connections to secure contracts (Transparency International, 2021, 14).

When it comes to the consideration of proliferation, then it is necessary to take into account the results of the mentioned research, especially the close ties between business and politics, because it is evident that business uses all available means to achieve its goals, which are primarily aimed at obtaining lucrative contracts with the state and the public sector, but it must also be borne in mind that there may be hidden goals, such as proliferation. The research shows that there is a dilemma regarding integrity, as well as that it is necessary to build integrity in both the public and private sectors (Transparency International, 2021, 5-7), which arises as an issue of particular importance when considering proliferation. It is precisely the lack of integrity and the placing of private interest above the public

one that can lead persons from the public and private sectors to hire companies or persons who can carry out proliferation for large projects. In such situations, the lack of integrity of persons involved in the public procurement process causes far greater problems through violation of procedures and regulations, as they can cause various forms of fraud, including proliferation (European Parliament, 2017, 70). In addition to the previously mentioned, it is necessary to bear in mind that the corruption of persons involved in large public projects represents a latent risk of proliferation that would be financed from national or EU funds.

An illustrative example of the abovementioned can be something that is otherwise a completely regular way of carrying out large complex projects, which is the engagement of contractors and especially subcontractors on large public projects. In the National Rules and the Need for a European Framework (European Parliament, 2017, 72), it was pointed out that the construction sector, as the eldest one affected by a wider use of subcontracting, has the most coverage of national rules. Also, besides the construction sector, the phenomenon of subcontracting chains has been reported in the facility management, transport, hotels, meat processing, healthcare and agriculture. The fact is that these industries are worker intensive industries, which elevate the risk of illegal workers, even migrants, and that could directly elevate the proliferation risk.

Hiring subcontractors carries a certain risk that starts with non-compliance risk, which can further manifest itself in the occurrence of fraud or the realization of more hidden goals, such as proliferation. When it comes to the risk of proliferation through subcontractors, it should be emphasized that there is also a risk in the services provided, such as maintenance. The risk refers to the huge potential that, through maintenance, it is possible to carry out proliferation, as well as the risk of persons performing such tasks, because persons working in maintenance can conduct proliferation as well. From the perspective of proliferation, it appears that, although there are specific hazards related to work, it also represents opportunities for proliferation through maintenance work, especially on large public and state projects.

In order to illustrate the risk of proliferation through subcontractors, as an example of a fraudulent scheme that can be suitable of proliferation, and at the

same time represents one of the quite frequent forms of subcontractor's fraud, is the so-called Social Dumping and Disappearing Subcontractors[38)]. Social Dumping is practice of employers to use cheaper labor than it is usually available at their site of production. In the first case, production is moved to a low-wage country or area, while in the second case, migrant workers are employed. The entrepreneurs will thus save money and potentially increase their profit. Disappearing Subcontractors are undertakings who are founded on a short notice in an EU member state, and are tasked with hiring workers in order to post them abroad. The workers begin working, the subcontractor is being paid, but refuses to pay his workers. If the workers claim their wages, the subcontractor disappears or goes bankrupt (European Parliament, 2017, 10-11).

Through these fraudulent schemes, proliferation can arise as a consequence of the purely economic interests of subcontractors and the desire to increase profits, which are otherwise the main cause of various fraudulent schemes. An additional risk is posed when subcontractors intend to commit fraud involving employees by hiring workers illegally, when, as a rule, there are no complete records of all employees, including security background checks. Therefore, taking into account all the above, it can be concluded that the lack of integrity and unprofessional behavior of subcontractors can allow persons who want to carry out proliferation to be engaged as cheap labor on large government and public projects, to carry out the actions necessary for proliferation and then disappear, together with the subcontractor.

All of the above is reflected or not reflected in business records in a certain way, and this is an area where accountants and auditors can identify indications of suspicion. Namely, accountants and auditors know the way how certain transactions are shown in business records and what the documentation trail looks like, so if certain deviations or absence of certain evidence are observed, it can be an indication to consider the suspicion of proliferation due to fraudulent schemes performed by the contractors and subcontractors.

[38)] In addition to the above, there are other fraudulent schemes, but these two are the most illustrative in the context of proliferation, so they are mentioned here.

CONCLUSION

The risk of proliferation of weapons of mass destruction is a reality that cannot be ignored; therefore, it is necessary for organizations to identify the risk of proliferation as a risk that can threaten the achievement of their goals and thus manage it and prepare a certain response to that risk. Although, from the entity's perspective, the risk of proliferation may appear to be minor, it should not be overlooked, because in certain industries or activities, it is quite real. Here, by the nature of things, the public and the state sector are imposed as sectors with a high risk of proliferation, in which it is necessary to establish clear mechanisms for identifying, managing and reducing this risk.

Having in mind that all illegal activities, including proliferation, are adaptable to the continuously changing environment, it is necessary to bear in mind that proliferation can be financed through financial sector by monetary means, but also through non-financial sector by non-monetary means. Due to this inevitable fact, we find that the FATF definition of financing proliferation needs to be expanded by adding the non-financial sector to financial services in order to get a comprehensive definition, which should be the following: Proliferation financing is providing financial support, either in monetary or non-monetary manner, for the transfer, conversion, export and use of nuclear, chemical or biological weapons, their means of delivery and related materials. At the same time, broadening of the proliferation financing definition expands the field in which proliferation can be identified and allows other professions, with their experts knowledge, to contribute to the identification and prevention of proliferation. Coordinated synergistic activities of DNFBPs from various fields can contribute to a timely recognition of the proliferation suspicion and use of the capacities that exist in other professions in the process of identification of proliferation, which should be the ultimate effect of the Public Private Partnership.

LITERATURE

1. Cindori, Sonja. 2017. *Recent Trends in Anti Money Laundering System: Proliferation of Weapons of Mass Destruction*, III International Scientific Conference Safety and Crisis Management – Theory and Practise Safety for the Future Proceedings. https://bekmen.rs.
2. EU Council. 2009. *European Security Strategy – A Secure Europe in a Better World*. https://www.consilium.europa.eu.
3. European Court of Auditors. 2014. *Can the EU's Centres of Excellence initiative contribute effectively to mitigating chemical, biological, radiological and nuclear risks from outside the EU?* Special Report https://www.eca.europa.eu.
4. European Parliament. 2017. Study for the JURI Committee, *Liability in Subcontracting Chains: National Rules and the Need for a European Framework*. https://www.europarl.europa.eu.
5. FATF/OECD. 2010. *Combating Proliferation Financing: A Status Report on Policy Development and Consultation*, Paris, France. https://www.fatf-gafi.org.
6. FATF. 2021. *Guidance on Proliferation Financing Risk Assessment and Mitigation*, Paris, France. https://www.fatf-gafi.org.
7. FATF. 2019. *Guidance for Risk-Based Approach – Accounting Profession*, Paris, France. https://www.fatf-gafi.org.
8. FATF. 2022. *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations*, Paris, France. https://www.fatf-gafi.org.
9. FATF. 2008. *Proliferation Financing Report*, Paris, France. https://www.fatf-gafi.org.
10. Transparency International. 2021. *Global Corruption Barometer European Union 2021 – Citizens' Views and Experiences of Corruption*. https://images.transparencycdn.org.
11. UN SC. 2004. *Resolution 1540*. https://www.un.org.

Mirsada Hukić*[)]

Mirza Ponjavić**[)]

Almir Karabegović***[)]

UDC: 004.89:[616.98:578.834-036.21(497.6)
004.89:614.2(497.6)

EPIDEMIC LOCATION INTELLIGENCE SYSTEM (ELIS): A MULTIDISCIPLINARY APPROACH FOR PREDICTION, EARLY DETECTION, TRACKING AND RESPONSE TO DISEASE OUTBREAKS

Abstract: *In Bosnia and Herzegovina, no joint public health institution has been established at the state level, but activities in this domain are the responsibility of the entities. For the purpose of spatial and temporal monitoring of the spread of the COVID-19 virus in Bosnia and Herzegovina, a research project was launched to establish an epidemiological location-intelligence system (ELIS) that supports the exchange of epidemic information between the entities and cantons. For its development, open-source software components present "in the cloud" were used as a working platform, equipped with all the necessary functionalities. The Epidemiological Intelligence System is intended for scientists, experts and professionals engaged in the field of health and other relevant areas participating in monitoring and research of epidemic phenomena, and it should be used to collect epidemic data, biostatistical analysis, evaluation of epidemiological surveillance systems, information, exchange of research data and reporting. The paper describes the role and potential of using ELIS as a research platform for health studies, including the experience gained in its application and directions for further development.*

Key words: *pandemics, intelligence systems, ELIS, platform, health*

*[)] Academy of Sciences and Arts of Bosnia and Herzegovina (ANUBiH).

**[)] International Burch University Sarajevo.

***[)] Electrical Engineering Faculty, University of Sarajevo.

INTRODUCTION

The launch of the Epidemic location-intelligence system (ELIS) project was motivated by the realization that, in Bosnia and Herzegovina, there is not a single system that would provide quality and timely information to healthcare institutions involved in solving health problems related to *COVID-19* and other epidemics in a unique way and for the entire country. This information is necessary for decision-makers on the implementation of various measures aimed at controlling the epidemic (procurement of protective equipment, tests, control of population movements, economic measures, etc.).

The subject of the research within this project is spatial and temporal monitoring of the spread of the *COVID-19* virus in the territory of Bosnia and Herzegovina through:

- collection of epidemiological and other data important for monitoring the occurrence of the epidemic and its spread,
- biostatistical analysis of the speed of spread and spatial-temporal distribution of infectious and other diseases,
- analysis and assessment of the epidemiological surveillance system, and proposing measures for its improvement,
- information, reporting and informing about the epidemic situation and evaluation of the effectiveness of control measures in order to make better decisions,
- evaluation of epidemic data through active serological surveillance and
- centralization and exchange of biostatistical and other data for research projects.

Throughout conducting this research, we have established an information and communication technology (ICT) infrastructure, as well as an application platform and data sets and models relevant for monitoring the spread of diseases and biostatistical analysis. As part of the epidemic information system, a geoportal was developed for geo-visualization, communication, data entry and search (Figure 1). The IT-communication component of ELIS, which includes a spatial database and a geoportal (Karabegovic & Ponjavic 2014, 27-40; Karabegovic et al. 2018), is intended for collection, analysis and exchange of geographic, health, statistical and environmental data. Its maintenance, application and development planning imply further research in the field of geoinformatics and geo-health.

This system is intended for scientists and professionals in the field of health and other relevant fields for monitoring and researching epidemic phenomena. The goal of its development is to provide information relevant to epidemic surveillance in Bosnia and Herzegovina, but also to establish a scientific-research database for other complementary and interdisciplinary projects.

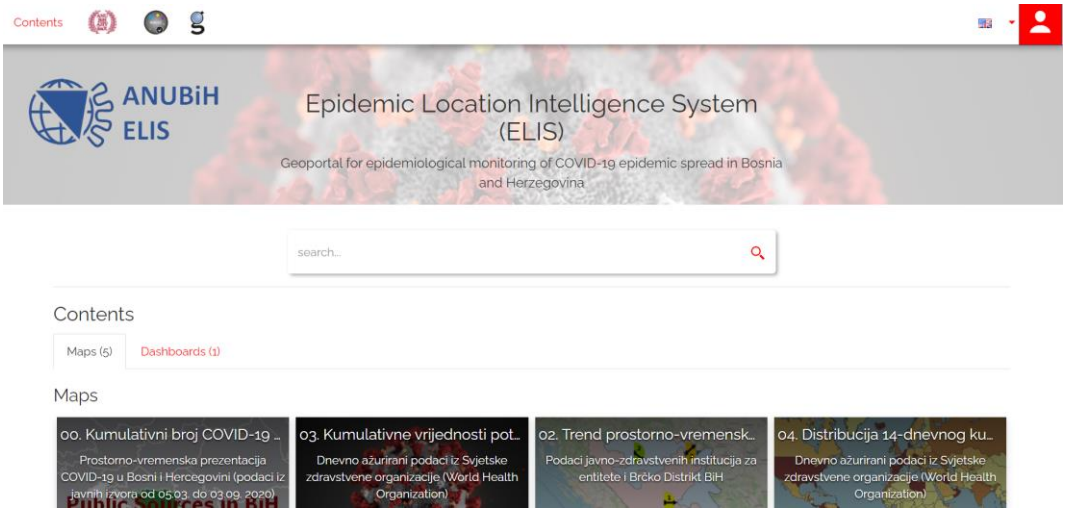


Figure 1 – Geoportal for geo-visualization, communication, data input and search (http://epidemija.gis.ba/)

1. ELIS USERS: FROM INTERDISCIPLINARY TO TRANSDISCIPLINARY RESEARCH

By combining health and geo-sciences, a wide spectrum of disciplines gathered around researching the dynamics of the earth and climate, the risk of exposure to their changes, and their impact on health, is covered. The potential of knowledge exchange between these disciplines (hydrology, seismology, geo-sciences, natural hazards, ecology, bio-sciences, veterinary medicine, human medicine) goes beyond traditional scientific cooperation and opens a collaborative space for the expansion and improvement of interdisciplinary research at the intersection of health, geo-science and environmental science.

The subject of interest in geo-health studies are cause-and-effect phenomena related to human health and the environment. Considering the connection between the natural world, human activities, climate and public health, the impact of all these factors on the spatial-temporal distribution and transmission of infectious and other diseases is evident.

The Center for Disease Control and Geo-health Studies is planned to conduct research through its sections for: health research, disease prevention and control, emergent/re-emergent zoonoses and bioterrorism, geospatial research and transdisciplinary research.

Therefore, within these sections, research groups are proposed for:

- laboratory diagnostics,
- clinical methods,
- epidemiology,
- geo-health studies,
- emergent/re-emergent zoonoses and unique health,
- biosafety and biosecurity.

These groups are supposed to establish interdisciplinary cooperation, so that each member of these groups is a potential user of ELIS. For example, research results and findings related to clinical methods can, like epidemic data, be spatially presented in the form of interactive maps, together with other related data. The goal of cooperation between groups and individuals from various fields is not only to combine knowledge and different approaches, but also to apply methods specific to other fields.

2. EXPERIENCES IN THE APPLICATION OF ELIS THROUGH RESEARCH RELATED TO *COVID-19*

So far, biostatistical methods have been applied and dynamic models have been developed for the analysis of data collected in the process of epidemic monitoring regarding the *COVID-19* pandemic. The dynamics of the spread of the virus in the population was monitored and the course of the epidemic was predicted. In this way, the spread of the infection was better understood, thus enabling us to conduct a more informative assessment of the epidemic situation and help in adopting more objective control measures.

The focus of the work was initially on IT development (i.e., infrastructure for the collection, centralization and analysis of data on the epidemic, with a server platform for Internet access and installed components that include a database, an application and a geoportal) and modeling of the phenomenon (i.e., spatial-temporal monitoring of the epidemic), and later on dissemination, education and informing the public. A network was established for the collection of epidemic data with public health institutes. It is worth noting that all the necessary official statistical data from the national statistics agency was entered into the database, and a complete IT infrastructure for ELIS was established.[39)]

[39)] The results of the project can be seen on the ANUBiH geoportal (https://www.anubih.ba/), and some of them are also published on the website of the European Association of Academies of Sciences – ALLEA (https://allea.org/).

Data were collected from various sources for different administrative levels and processed with biostatistical methods, and the results were reported on the ELIS geoportal (Figure 2).

Mechanisms for data exchange between health institutions and the project team for the analysis and evaluation of epidemiological data have been improved. The Geoportal, which is the entry point for accessing all information and data from the database, is accessed through the official website of ANUBiH. By implementing components for input, biostatistical modeling and epidemic reporting, a faster flow of information from the epidemic surveillance system was established, and more transparent access to information was enabled for decision-makers, epidemic teams and citizens. The current dynamics and the scale of the *COVID-19* epidemic, as well as the elevated need for more efficient management of the health crisis, require its further development, upgrading and maintenance.

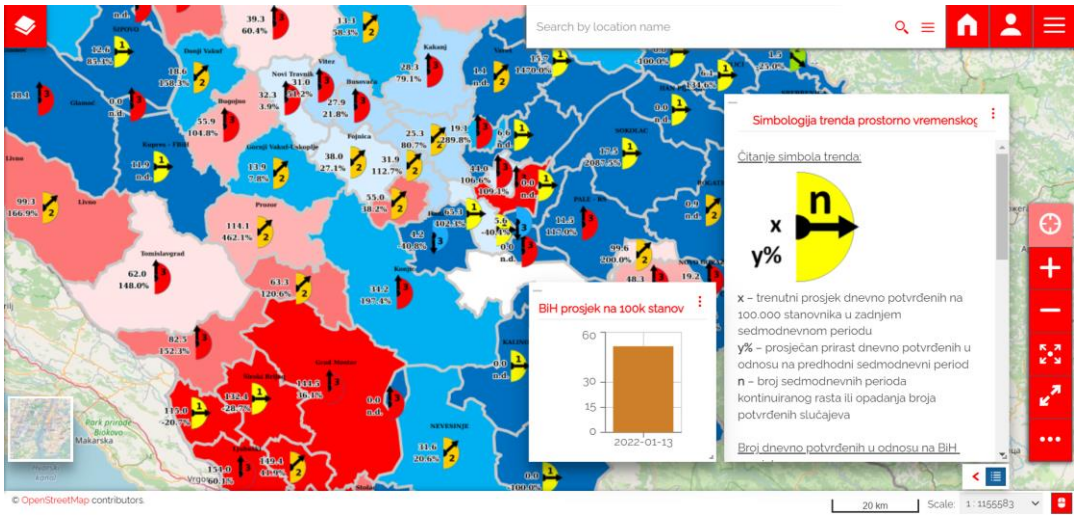


Figure 2 – ELIS geoportal: modeling and geo-visualization of collected data

3. SYSTEM UPGRADE AND FURTHER FUNCTIONAL DEVELOPMENT

During implementation of ELIS, the need for equipping it with a mechanism for automated collection and entry of data into the system, as well as an improved method of geo-visualization, was recognized. Therefore, the development of new software modules for the acquisition and spatial presentation of epidemic data was set in motion with the aim of speeding up the entry and enabling easier access of information regarding the pace of the spread of *COVID-19* on the Internet.

The available data sources were analyzed and the types of their heterogeneity were recognized (Coetzee et al. 2020, 90), including:

- data format (data are displayed through a web application, as HTML, and as daily reports in PDF format);
- data structure (they are presented as standard text, structured in tables, and by graphs);
- structure stability (some data sources are not reported according to established patterns, but their structure changes over time);
- administrative level of data (data from different sources are displayed at different levels: municipality, canton, district, entity, national);
- data grouping method (one data source can have all data grouped as one document or several documents);
- data addresses (some data sources have a static link that does not change, others have links that change over time) and
- language and script (data can be written in Latin or Cyrillic letter).

Based on the previously presented typology, the challenges for automation of downloading and transformation of data from available sources were recognized (Ponjavic & Karabegovic 2019, 13). Existing available software solutions were analyzed and none was found that could provide an answer to all the previously mentioned challenges (Helmi et al. 2018, 145-158). That is why it was decided to develop a new software module that will include the necessary mechanisms and be upgradeable in terms of future changes and requirements.

In accordance with the planned functional development, a tool was designed that helped us establish a complete ETL (Extract-Transform-Load) procedure for the automatic population of the ELIS database, including:

- data format recognition:
  - well-structured data sources or web applications, where it is possible to obtain data as a web service (most often in JSON data format);
  - daily reports in the form of a PDF document on the web;
  - other text sources, such as HTML pages, with the application of a text reading mechanism;
- data transformation, depending on their structure:
  - the web service uses the JSON tool for conversion to the ELIS database;
  - additional library licensed as open-source under AGPL (iText for reading PDF documents) is used for documents;
  - for other text sources, such as HTML pages, a text reading mechanism has been developed;
- establishment of a database of previous structures (due to the variability of the data structure, a trial-and-error database was established so that the system remembers previously recognized structures and tries to apply them until it finds a suitable one);
- establishment of a dictionary for data levels that contains all levels with their relationships (higher or lower), and different names per level (i.e., municipalities in different sources may have different names);
- establishment of a database of data groups (e.g., the mechanism remembers the previous data grouping and tries to apply it, and if it does not get the expected result, then it tries the next form);

- establishment of the link database (e.g., the mechanism remembers the applied links and tries to use them, and if it does not get the expected results, then it tries the next ones from the list);
- creation of a mechanism for the transformation of the alphabet - due to the dual use of alphabets, a mechanism is used for the conversion of the Cyrillic alphabet into Latin alphabet and vice versa.

4. APPLICATION OF ELIS AS A TOOL FOR ESTABLISHING A DIGITAL ATLAS OF REGISTERED INFECTIOUS AND NON-INFECTIOUS EPIDEMIC DISEASES IN BOSNIA AND HERZEGOVINA

As an important resource, but also as a platform used in the processes of development of research projects, the scientific-research database of the epidemic location-intelligence system (ELIS) is deemed as a platform that has great potential (Hukic et al. 2020, 111-116; Ponjavic et al. 2020). In this sense, the need to use ELIS through its further application as a tool for establishing a digital atlas of registered infectious and non-infectious epidemic diseases in Bosnia and Herzegovina was recognized. The benefit of such an atlas would be manifold. In addition to being used for education, it would serve as useful in presentation of the distribution of the disease, and would thus contribute to better understanding their location-related factors. A cartographic presentation would better describe the occurrence and spread of the disease, and the maps would serve as a useful research tool to present the acquired information, as well as various hypotheses related to the location of the occurrence of the disease (Hukic et al. 2021, 111-116). This would enable projections of the further occurrence of the disease with the use of further identifiers about residents and their migration, habitats of certain animal species, as well as knowledge about pathogens, their vectors, reservoirs, but also general data about the physical, chemical and ecoclimatic environment.

CONCLUSION

The main goal of the ELIS project is to contribute to the efficiency of epidemic surveillance and implementation of more effective infection control measures in Bosnia and Herzegovina by establishing a research database. This was achieved through the development of an application platform and the establishment of a database with models relevant for monitoring the spread of disease and biostatistical analysis. An important part of the system is the geoportal, which was developed for geo-visualization, communication, input and data search. As such, the geoportal has the role of an access point for the use of epidemic, ecological, statistical and spatial data. In addition to application support for communication and cooperation of all public health institutions and the public, it enables analysis, geocoding of confirmed cases of COVID-19, identification of disease dynamics, identification of vulnerable groups, mapping of health capacities and general modeling of the spread of infection. The current dynamics and scale of the COVID-19 epidemic, as well as the need for efficient management of the health crisis, require its further development, upgrading and maintenance.

In addition to the geoportal, the ELIS database has great potential for establishing a digital atlas of registered infectious and non-infectious epidemic diseases in Bosnia and Herzegovina. If applied with demographic identifiers, physical, chemical, ecoclimatic, biological and other data, this kind of scientific-research base could be used to identify various patterns important for predicting the occurrence of diseases.

REFERENCES

1. Karabegovic, A.; Ponjavic, M. 2014. Geoportal as Interface for Data Warehouse and Business Intelligence Information System. *Advances in Intelligent Systems and Computing Advances in Business ICT*.
2. Karabegovic, A.; Ponjavic, M.; Ferhatbegovic, E.; Karabegovic, E. 2018. Spatial Data and Processes Integration in Local Governance of Bosnia and Herzegovina. *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*.
3. Coetzee, S.; Ivánová, I.; Mitasova, H.; Brovelli, M. 2020. Open Geospatial Software and Data: A Review of the Current State and A Perspective into the Future. *ISPRS International Journal of Geo-Information*, *9* (2), 90.
4. Ponjavic, M.; Karabegovic, A. 2019. Location Intelligence Systems and Data Integration for Airport Capacities Planning. *Computers*, *8* (1), 13.
5. Helmi, A. M.; Farhan, M. S.; Nasr, M. M. 2018. A Framework for Integrating Geospatial Information Systems and Hybrid Cloud Computing. *Computers & Electrical Engineering*, *67*, 145–158.
6. Hukic, M.; Ponjavic, M.; Tahirovic, E.; Karabegovic, A.; Ferhatbegovic, E.; Travar, M.; Serdarevic, F. 2021. SARS-CoV-2 Virus Outbreak and the Emergency Public Health Measures in Bosnia and Herzegovina: January – July, 2020. *Bosn J of Basic Med Sci*.
7. Ponjavic, M., Karabegovic, A., Ferhatbegovic, E., Tahirovic, E., Uzunovic, S., Travar, M., Pilav, A., Mulic, M., Karakas, S., Avdic, N., Mulabdic, Z., Pavic, G., Bico, M., Vasilj, I., Mamic, D., & Hukic, M. 2020. Spatio-temporal data visualization for monitoring of control measures in the prevention of the spread of COVID-19 in Bosnia and Herzegovina, *Medicinski glasnik*, 17(2). https://doi.org.

Velas Andrej*)
Durica Jakub**)
Boros Martin***)

UDC: 347.72:[005.52:005.334
347.72:[616.98:578.834-036.21(437.6)

THE ROLE OF SECURITY MANAGEMENT IN PROTECTING COMPANIES DURING A PANDEMIC

Abstract: *The article includes a description of security solutions in commercial companies during a pandemic. The solutions are also applicable in critical infrastructure or other facilities. Security managers form a specific part of management and do not bring direct profit to companies, but they ensure the continuity of activities in the company. Their goal is a state without security incidents. If there are no or minimal security incidents, top management often sees security as one of the options where savings can be made. The situation related to the COVID-19 pandemic has brought new tasks and competences for security managers in enterprises. Most of them became members of the crisis staffs in the enterprises and thus also fulfilled crisis management tasks.*

Key words: *security management, pandemic, COVID-19, comapny protection.*

INTRODUCTION

Security management is a specific management activity, aimed at managing the security of a reference object, and thus represents a type of human work, one of the most important human activities, which enables all activities to be carried out safely in the object that is subject to the protection in question. Security management nowadays is percieved as a highly specialised security management activity that no larger organisation can do without. In its most general terms, it can be characterised as the sum of all the activities that need to be done to achieve, ensure and consolidate the security of people, property and the environment of an organisation. This activity constitutes the security management process of the organisation (Belan 2015). According to Ntouskas (2012), security management is

*) PhD in Philosophy, Professor of the University of Žilina, Department of Security Management; Zilina, the Slovak Republic.
**) Master of Engineering, University of Žilina, Department of Security Management; Zilina, the Slovak Republic.
***) Assistant Professor at the University of Žilina, Department of Security Management; Zilina, the Slovak Republic.

a continuous and systematic process of identifying, analysing, processing, reporting and monitoring an organisation's operational risks. Security management is an important process of management and control aimed at protecting an organisation from both internal and external risks that could negatively affect the achievement of its operational goals. Heyerdahl (2022) likewise says that security management is aimed at protecting against negative acts. Managing an organisation's security requires the latest technology and a high level of security awareness and education for all employees to reduce risk (Shammari 2021).

Over the several past decades, the position of security manager in an organisation has risen from the bottom to the top ranks in any company or similar type of organization. As a result, security managers report directly to top management, if not to the CEO. Often we can find security managers in the roles as high as the positions of vice presidents of security or chief security officers. This is the result of the importance of security having come to the fore in the private sector as well (Sennewald 2020). Security managers are the people who have the responsibility for the creation, implementation and operation of the Security Management System. In the field of security, they are also responsible for:

- senior managers – e.g. CEO, HR Director, CFO, CIO, CTO, corporate lawyer, etc,
- ine managers - responsible for security in their departments.

Security managers themselves manage security. This includes the following positions: security manager, risk manager, cyber security manager, fire protection technician, fire protection specialist, security technician, authorised security technician, occupational health practitioner, physical protection manager and others.

The competencies of security managers are the following:

- individual skills of security managers, such as organizational skills, ability to communicate with people, public speaking, ability to make informed decisions, etc,
- intuition, creativity, the ability to anticipate and take risks at the right moment when applying management tools, techniques and principles,

- the ability to seek appropriate opportunities to improve the security management system and influence the security of the organisation,
- the ability to build a capable team of security personnel in the organisation's security management system, and
- the ability to create a vision for the security of the organisation, to find opportunities where others see only chaos, contradictions and conflicts.

The priority task of security management is the protection of company assets. Essentially, we are talking of physical protection, aimed at external and internal security threats. Based on surveys conducted in several companies, we have found that security managers have cumulative competences in other areas (occupational health and safety, fire protection, civil protection, personal data protection, etc.) They are deemed as pivotal players among the company staff given that they participate in business continuity management and thus ensure proper functioning of a company. The position of security manager is specific to each company and is profiled as the company evolves. Security managers are often based in human resources or other departments. It is generally known that security managers and the security department do not generate any profit for companies; on the contrary, they protect the company from losses, thus serving their purpose. Therefore, it is important for security managers to be able to present the results and importance of their department to the company director (Magestro 2019). In terms of the role of security in an organization, we can divide it into the following categories:

- The protective service role – this is the most visible function in the security department. This role is usually given to the posts that serve as protectors or guardians, who are tasked with protecting all the property and all the people who employed with the given company.
- Specific services – security management, which understands the rationality and logic of providing the widest possible range of special services, thus advancing the security function, necessary in every company or enterprize.

The specific services in question can further be divided into the following categories:

- Investigative assistance – use of investigative skills in peripheral services;
- Bodyguard/escort service – duties of the bodyguard provided by the company. Usually this is the function of a personal chauffeur, escorting company guests; and
- Emergency service – it is a centre for handling emergency messages, dispatching emergency services, alerting relevant persons to problems.

- Educational services – nowadays, the educational function is coming to the forefront of the security department, due to elevated need for asuring the implementation of law sand order in any given company.
  - General security programs – training of new employees arose as quite a necessity in the modern times of security management. The task of individuals engaged with conducting educational security programs is to create general security regulations that are focused on understanding the goals of the security department;
  - Supervisory training sessions – supervisor training, focused on supporting supervisors in their new responsibilities, is the first stop in educating the staff;
  - Employee self-protection programs – Programs for self-protection and prevention of violent crime; and
  - Unit or departmental presentations – creation of special presentations designed for individual departments as a result of better and more precise definition of security, processes depending on the tasks of the department.
- Management services – Security department managers should also be in the company's leadership team in order to achieve better results in the overall security of the organization (Sennewald 2020).

1. COVID-19 PANDEMIC

SARS-CoV-2, known as *COVID-19*, was first identified during the Chinese New Year celebrations. Initially, the virus was thought to have originated at animal markets, which are very popular in the People's Republic of China. Subsequently, the virus spread from China to the rest of the world, triggering a pandemic called the *Covid-19* pandemic (Rahimi 2020). The pandemic has become a world-wide menace, resulting in more than 500 million infected and 6.4 million dead, according to statistics as of August 2022. In addition to the severe impacts on people's health and overstretched health services, the *COVID-19* pandemic is also impacting the economies of entire countries world-wide. The functioning of the companies as participants in the company did not escape the effect of the pandemics as well, which is important due to the fact that such entities generate a country's gross domestic product. As a result of the pandemic, there has been an economic crisis, which severity is often compared to that of 1929 (McKee 2020; Bansal 2020; Ceylan 2020). The first confirmed case of *COVID-19* has been detected in Slovakia on March 6, 2020 (PHAoSR 2022). As a result of keeping companies open, the security managers employed in these companies were faced by a number of challenges emerging as the result of the *COVID-19* pandemic. Prior to the pandemic period, few enterprises had crisis scenarios and methodological procedures in place to deal with a similar situation, which made the current situation more difficult. Even those that were prepared had difficulty purchasing the necessary materials to ensure production and maintain the safety levels of their own employees.

Security managers in Slovakia had workshops on the above issue and looked for common solutions. Cooperation and exchange of experience is very important for dealing with emergency situations. It is important to share information on the availability of detection technologies and how to carry out preventive activities.

According to a survey conducted at the Security Managers Workshop in the Slovak Republic in June 2022, at the time the workshop took place, a total of 99% of companies already had guidelines for pandemic situations. However, during the pandemic period, successive incoming issues were addressed in discussion forums. The Association of Security Managers has been active in Slovakia since 2017 and brings together professionals working in the commercial security market in private companies. It is estimated that there are approximately 80 such positions in companies in Slovakia, with up to 30 members and associate members regularly attending the workshops (SABM 2022).

However, in the first phases of the pandemic, the security managers proceeded intuitively and decided to exclude the risk management process. The Government of the Slovak Republic and the Public Health Authority of the Slovak Republic also contributed to the management of security in companies, through the issuance of several decrees to prevent the spread of the infectious disease *COVID-19*. The first measures, taken in January and February 2020, was directed towards all the passengers who arrived to Bratislava from Italy; these passengers were at the time of their arrival checked for their health status. On February 27, 2020, the Security Council of the Slovak Republic met in order to discuss the issue of the *COVID-19* disease and consequently decided to introduce the first measures (PHAoSR 2020). As the first measure to prevent the spread of *COVID-19*, which also affected businesses, the Measure of the Health Authority of the Slovak Republic n. OLP/2732/2020 and Slovak Government Resolution No. 174 was introduced on March 23, 2020, imposing mandatory covering of the upper respiratory tract with masks. There was a shortage of face masks on the market, to which security managers responded by contracting supplies of face masks from individual manufacturers. It was also recommended to measure the temperature at the entrance to the workplace. The temperature taking and health checks raised questions about data protection, and therefore, the Opinion of the Chair of the

Committee on the Council of Europe Convention 108 and the Council of Europe Data Protection Commissioner on personal data in the context of the COVID-19 pandemic was issued, stating the following: "In accordance with Convention 108, it is crucial, that even in particularly difficult situations, data protection principles are respected and therefore it is ensured that data subjects are made aware of the processing of personal data related to them; processing of personal data is carried out only if necessary and proportionate to the explicit, specified and legitimate purpose pursued; an impact assessment is carried out before the processing is started; privacy by design is ensured and appropriate measures are adopted to protect the security of data, in particular when related to special categories of data such as health related data; data subjects are entitled to exercise their rights" (Pierucci 2020). In the first days after the introduction of this measure, there was a shortage of digital non-contact thermometers on the market. However, the distance between the individuals that were subjected to temperature measuring and the person taking the measurement, and thus the possibility of emergence of the resulting hazards, were problematic. Thermal imaging cameras were massively used at that poiny, which made it possible to increase the distance between operators and to automate the measurements and link them to a system restricting access to persons with elevated temperatures (turnstiles, culverts). The cost of thermal cameras has increased several times, but temperature measurement has not produced the desired results and its efficiency had been low. Rather, it had a preventive function, where persons with elevated temperature or with symptoms of *COVID* were instructed to return and stay at home as a precaution (Velas 2020). Temperature measurement at the entrance to the building has also been introduced by the Faculty of Security Engineering of University of Zilina, during the final state exams in 2020. The results showed that only one person didn't meet the requirements for access to the building. However, the person showed a valid negative test and was allowed to enter, thus raising a question regarding the

validity of the testing. The conclusions of these measurements were that it is advisable to use an electronic access control system in combination with a thermal imaging camera. A QR code reader, commonly used in electronic access control systems, can be used to prove negativity (Durica 2022). Another option is to use *RFID* cards, on which the employee's health information will be recorded. If the health status is satisfactory, the electronic access control system will be activated and the employee will be allowed entry. Consequently, distances between co-workers as well as between employees and customers were introduced according to the Measure of the Health Authority of the Slovak Republic n. OPPL/2742/95916/2020. In industrial companies, there had been problems related to the entry of large numbers of employees. For example, in the automotive industry, where several thousand employees came in at once for a shift within 20 minutes, delays occurred. This was a direct result of the cost of barrier systems, as well as of the issue of marking appropriate distances, etc. At *UNIZA* (University of Zilina), we studied the issue of throughput of RFID readers, i.e. the number of possible readings of cards or chips per minute.

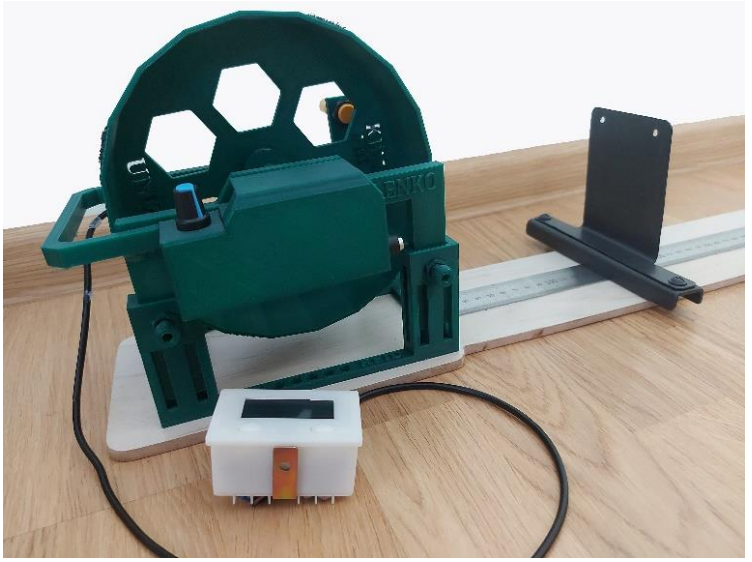


Figure 1 – Equipment for measuring the throughput of RFID readers

Entry corridors in companies needed to be set up in such a way that contacts between employees were kept to a minimum. Currently, a project to monitor the movement of employees in the company through RFID technology is being addressed and examined at UNIZA. The advantage of the system is the tracking of contacts with a positive person, which is quite complicated (Lenko 2021).

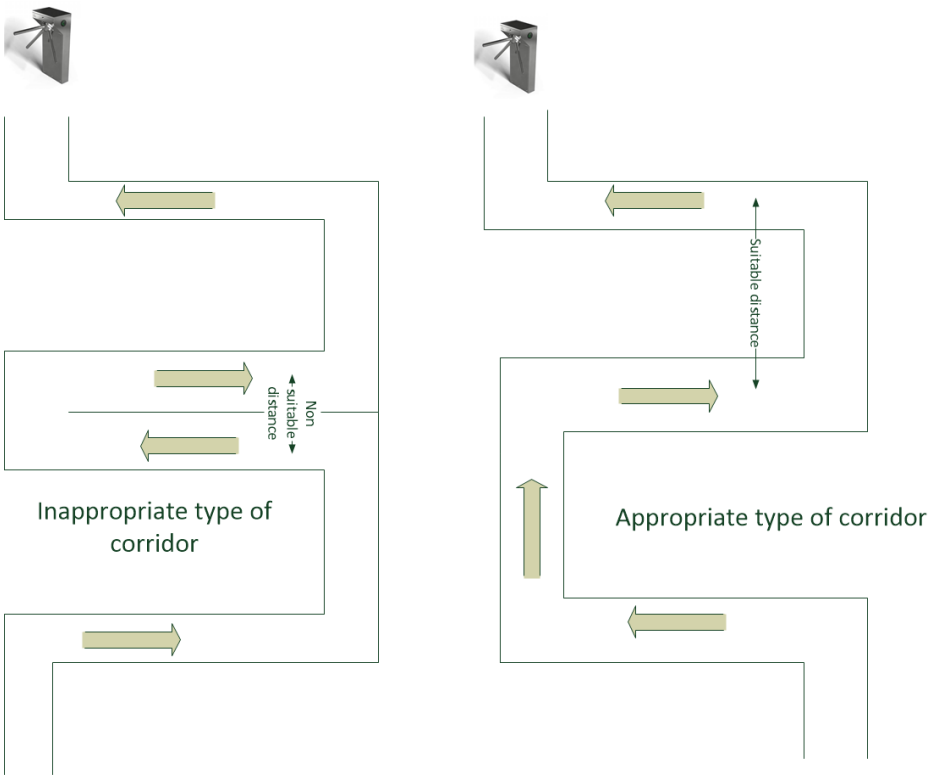


Figure 2 – Correct and wrong way of creating corridors in front of access control systems

The Slovak Government, in accordance with the associated Home Office, introducted the Government Resolution No. 49/2021, thus introducing a curfew for all individuals employed in positions with nature which enables such actions to be implemented. However, this arose the need for introducing the additional administrative activity of checking whether the staff were fulfilling their duties

while working at home. Moreover, it is worth noting that the security managers had to secure the premises that were abandoned by the said staff. This entailed an increase in the cost of security guards. A specific feature of the security service (protection of premises) is that the work cannot be carried out in the form that would be in line with the beforementioned Resolution, and thus from a home office.

2. METHODOLOGY

The theoretical foundations of the security manager's tasks were the best described by Belan in his work entitled "The theory of security management". Moreover, a specific approach has been taken by Hofreiter (2015), who links the activities of security managers to the safety culture. The activities of security management are subject to professional competence. Such education is provided by the University of Žilina, but the positions of security managers are held by graduates of different schools with different approaches to security management. Specialised courses on security management are provided by ASIS. However, these do not take into account the specificities and legislation of the particular country where the security manager operates. To identify the roles of security managers during the *COVID* pandemic, we used a simple face-to-face survey. It was subsequently supplemented and modified based on the in-person brainstorming during the security managers' workshop. The competencies themselves have been and are being monitored by members of the Department of Security Management from the beginning of the pandemic until the present times, with the support of the project VEGA 1/0173/21 – Research of measures implemented by security managers in the organizations related to the occurrence and spread of *COVID-19*. Therefore, it is worth noting that only publications by authors from the Department of Security Management deal with the issue of security management during *COVID* and its specifics.

3. RESULTS

The basic tasks in ensuring business continuity in the company were the following activities, as they were defined by 24 security managers of selected companies in Slovakia while brainstorming at a workshop held in 2021:

- checking for certificates of testing or vaccination,
- wearing a face mask,
- implementing disinfection measures,
- maintaining the rule of physical distancing,
- incouraging work from home, and
- checking the body temperature.

Currently, security managers in Slovakia are primarily guided by the *COVID* Automated Response, issued by the Ministry of Health of the Slovak Republic, which is introduced at the point when the World Health Organization (WHO) declared a pandemic in the Slovak Republic. The Automated Response is based on weekly monitoring (every Monday) of the number of positive cases and the determination of measures depending on the growth, that is, the decline of cases of infected individuals.

			Level of Threat		
Grade	Monitoring	Vigilance	1st level	2nd level	3rd level
Balanced 7-day incidence	Growth: (0-10) Decline: (0-20)	Growth: (10-50) Decline: (20-150)	Growth: (50-150) Decline: (150-300)	Growth: (150-250) Decline: (300-500)	Growth: >=250 Decline: >500
Face mask/FFP2 respirator	face mask in the interior and at the mass event also in exterier	face mask in the interior and at the mass event also in exterier	required respirator in interior and face mask in exterior with some exceptions up to 2 m distance	required respirator in interior and in exterior up to 2 m distance	required respirator in interior and in exterior up to 2 m distance
Entry to company/firm	without restrictions	without restrictions	vaccinated/tested /after COVID	vaccinated/tested /after COVID	vaccinated/tested /after COVID

Figure 3 – *COVID* automat (Korona.Gov 2022)

The implementation of the *COVID* automat moves the responsibility for restrictions in companies to the state, but the possibilities for refunding the costs associated with the measures are minimal. This leaves the security managers with free hands to prioritise the protection of the company property and the attributed assets. The stabilisation of the situation after four pandemic waves has resulted in a relaxation of measures, with the next pandemic wave, at the moment of writing this research paper, expected in autumn 2022. Compared to the previous waves, which occurred in a relatively short succession, the security managers have set up a system of measures, created documentation to deal with *COVID*-related incidents, as well as purchased the necessary equipment in order to cope with the next wave of the pandemic.

The current pandemic is likely to fade, but the future waves of *COVID-19* outbreaks, that are most possibly going to be potentially seasonal, may occur (Branswell 2020; Joseph 2020; Lipsitch 2020). Any upcoming outbreak is expected to raise serious concerns among public health authorities, health workers, politicians and the general public (Joseph 2020, Goodman 2020, 16). Moreover, it is necessary stressing that the countries affected by the *COVID-19* outbreak throughout the world have responded differently, but a unified strategy is needed to tackle this pandemic. Time will tell if they can handle the situation or not in a proper way.

CONCLUSION

The *COVID-19* pandemic brought along the new challenges and issues that security managers had are are still having to deal with. These situations were neither planned nor expected. No procedures were in place to deal with the problems arising from the anti-pandemic measures. Therefore, in the beginning, most security managers relied on themselves and their intuition to protect the

assets and profits of the business they are employed with. The role of physical protection of facilities, in this context, is primarily to protect the assets. Nevertheless, the pandemic touched every security manager. The article was constructed in a way so that it provides a description of the challenges that security managers in enterprises had to deal with, as well as the ones that will be present in the future, given the expected new waves of the *COVID* pandemic. The security managers' roles were identified through personal interviews and brainstorming sessions at Security Managers Association seminars, as we have previously mentioned.

Finally, we would like to acknowledge and stress that this research was funded by the Scientific Grant Agency of the Slovak Republic, grant number VEGA 1/0173/21, intended towards research linked to the project of Research of measures implemented by security managers in the organizations related to the occurrence and spread of *COVID-19* and in other emergency situations. The project, that is, this research, was also supported by a grant given by the Slovak Research and Development agency, grant No. APVV-20-20676, referred to the project entitled "Monitoring and tracing of movement and contact of persons in medical facilities".

REFERENCES

1. Bansal Tanmay. 2020. Behavioral finance and COVID-19: Cognitive errors that determine the financial future. SSRN. http://dx.doi.org.
2. Belan Ľubomír. 2015. Bezpečnostný manažment. Manažérstvo bezpečnosti. Žilina: EDIS – vydavateľstvo Žilinskej univerzity.
3. Branswell Helen. 2020. We're learning a lot about the coronavirus. It will help us assess risk. Stat. https://www.statnews.com.
4. Ceylan Rahmiye Figen, Ozkan Burhan, Mulazimogullari Esra. 2020. Historical evidence for economic effects of COVID-19. Nature Public Health Emergency Collection. https://10.1007/s10198-020-01206-8.
5. Durica Jakub, Velas Andrej, Soltes Viktor. 2022. Management of final examinations during the pandemic COVID-19. 14th annual International Conference on Education and New Learning Technologies.
6. Goodman Brenda. 2020. Flood of COVID-19 Patients Could Swamp Hospitals. Medscape. https://www.medscape.com.
7. Heyerdahl Anne. 2022. From prescriptive rules to responsible organisations – making sense of risk in protective security management – a study from Norway. European Security. https://doi.org.
8. Hofreiter Ladislav. 2015. Manažment ochrany objektov. Žilina: EDIS – vydavateľstvo Žilinskej univerzity, 2015, ISBN 978-80-554-1164-4
9. Joseph Andrew. 2020. Coronavirus spread could last into next year, but impact could be blunted, CDC official says. Stat. https://www.statnews.com.
10. Korona.Gov 2022. Covid Automat. https://korona.gov.sk.
11. Lenko Filip. 2021. Specifics of RFID Based Access Control Systems Used in Logistics Centers. Transportation Research Procedia Volume 55. https://doi.org.

12. Lipsitch Marc, Swedrdlow L David, Finelli Lyn. 2020. Defining the Epidemiology of Covid-19 – Studies Needed. The New England Journal of Medicine. https://10.1056/NEJMp2002125.

13. Magestro Brandon. 2012. Transitional Phase of a Security Manager: A Closer Look into the Struggles and Difficulties Experienced during the Transition into Security Management. Journal of Applied Security Research. http://dx.doi.org.

14. Measure of the Health Authority of the Slovak Republic n. OLP/2732/2020.

15. Measure of the Health Authority of the Slovak Republic n. OPPL/2742/95916/2020.

16. McKnee Martin, Stucker David. 2020. If the world fails to protect the economy, COVID-19 will damage health not just now but also in the future. Nature Medicine 26. https://doi.org.

17. Ntouskas Theodoros, Pentafronimos George, Papastergiou Spyros. 2011. STORM – Collaborative Security Management Environment. Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication. https://doi.org.

18. PHAoSR. 2020. COVID-19: Conclusions of the Security Council meeting. https://www.uvzsr.sk.

19. PHAoSR. 2022. Two years since the first confirmed case of COVID-19. https://www.uvzsr.sk.

20. Pierucci Alessandra, Walter Jean-Philippe. 2020. Statement on the right to data protection in the context of the COVID-19 pandemic. https://www.coe.int.

21. Rahimi Farid, Abadi Bezmin Talebi Amin. 2020. Tackling the COVID-19 Pandemic. Archives of Medical Research Vol. 51, Issue 5. https://doi.org.

22. Sennewald A. Charles, Baillie Curtis. 2020. Effective Security Management 7th edition. Elsevier: Butterworth-Heinemann.

23. Shammari Ayla Al, Maiti Richard Rabin, Hammer Bennet. 202. Organizational Security Policy and Management during Covid-19. SoutheastCon 2021. https://doi.org.

24. Slovak Government Resolution No. 49/2021. VYHLÁŠKA Úradu verejného zdravotníctva Slovenskej republiky, ktorou sa mení vyhláška Úradu verejného zdravotníctva Slovenskej republiky č. 45, ktorou sa nariaďujú opatrenia pri ohrození verejného zdravia k obmedzeniam prevádzok a hromadných podujatí; Vestník vlády Slovenskej republiky, Čiastka 21/2021.

25. Slovak Government Resolution No. 174 of March 23, 2020. 174/2020 Z. z. OPATRENIE Ministerstva práce, sociálnych vecí a rodiny Slovenskej republiky.

26. Velas Andrej, Flodr Martin. 2020. Problematika merania telesnej teploty osôb v súvislosti s ochorením COVID-19. In: Civilná ochrana: revue pre civilnú ochranu obyvateľstva.

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

355.02:005.334(062)

INTERNATIONAL scientific conference (2022 ; Cavtat–Dubrovnik)
How to deal with uncertainties in increasingly complex environment?
: (the new cartography of risk and crises) : proceedings of the international scientific conference held in Cavtat – Dubrovnik September 27-29, 2022 / [editors Zoran Keković, Ratko Duev, Jadranka Polović]. - Skopje : Faculty of philosophy – Institute for security, defense and peace "Ss. Cyril and Methodius" university ; Belgrade : Center for risk analysis and crisis management (CARUK), 2023. - 296 стр. : илустр. ; 30 см

Фусноти кон текстот. - Библиографија кон трудовите

ISBN 978-608-238-233-3 (Faculty of philosophy) ISBN 978-86-902810-4-6 (Center for risk analysis and crisis management
(CARUK))

а) Безбедност -- Предизвици -- Собири

COBISS.MK-ID 60753669

ISBN 608238233-1