INTERNATIONAL CONFERENCE SAFE AND SECURE SOCIETY 2024

Ceske Budejovice, October 9. – 10., 2024
Czech Republic

CONFERENCE PROCEEDINGS

Ceske Budejovice 2024

The College of European and Regional Studies
Department of Law and Security Studies

Publisher:
The College of European and Regional Studies
Czech Republic

Edited by:
PhDr. Štěpán Kavan, Ph.D.

https://doi.org/10.36682//SSS_2024
ISBN 978-80-7556-151-0
ISSN 2533-6223 (online: www.icsss.eu)

PROGRAMME AND SCIENTIFIC COMMITTEE

Denis K. Alexeev
Russian State Hydrometeorological University, Saint Petersburg, Russian Federation

Ali Asgary
Faculty of Liberal Arts and Professional Studies, York University, Canada

Tom Børsen
Center for Applied Ethics and Philisophy of Science, Aalborg, Denmark

George Boustras
European University Cyprus, Nicosia, Cyprus

Lenka Brumarová
Faculty of Safety Engineering, VŠB – Technical University of Ostrava, Czech Republic

Andrea Čajková
Faculty of Social Sciences, University of Saints Cyril and Methodius, Slovak Republic

Leonor Calvo
Department of Biodiversity and Environment Management, University of Leon, Spain

Jiří Dušek
College of European and Regional Studies, Czech Republic

Benoît Flamant
Fire Rescue Service of Savoy Department, France

Igor Goncharenko
University of Civil Protection, Ministry for Emergency Situations of the Republic of Belarus, Republic of Belarus

Zdeněk Hon
Faculty of Biomedical Engineering, Czech Technical University, Czech Republic

Radoslav Ivančík
Academy of the Police Force in Bratislava, Slovac Republic

Katharina Anna Kaltenbrunner
Department of Strategic Management and Organization, Faculty of Law, Paris Lodron University of Salzburg, Austria

Štěpán Kavan (chairman)
Fire Rescue Service of South Bohemia, Faculty of Health and Social Sciences, University of South Bohemia, Czech Republic

Rastislav Kazanský
Faculty of Political Science and International Relations, Slovak Republic

CONTENT

PREFACE

Safe and Secure Society 2024 Conference Proceedings contain selected and revised papers from the 8th International conference. Safe and Secure Society 2024 Conference was held as an "in-person" konference on October 9. – 10., 2024.

The conference provides a platform for meetings of experts dealing with security issues at regional, national and international level. The conference focused on:

- Getting familiar with the practical experience of each organization in emergencies associated with the “human” element.
- Comparing current approaches to dealing with emergencies on “human” element topic in terms of crisis management, rescue and psychosocial assistance, presenting the possibilities of involvement of non-governmental non-profit organizations, international assistance and development cooperation.
- Creating space for people, communities, and organizations to come closer together.

We are pleased to introduce you the proceedings from the conference on security and safety issues. We follow up the previous proceedings focused on the topic of security and safety. Therefore we had to refuse some authors. We also made the conditions of review process stricter, which led to increasing quality of published articles, in our opinion. We believe that you will find different views of the topic on safe society in all its complexity, and useful information on it as well.

We also submit the proceedings as a platform for establishing new work contacts which are inevitable for future development of the security issue. We are pleased that the publications from previous conference attract general interest. The number of participants, which is high every year, is important to us as well.

We will be glad if the proceedings is for you a memory of this year’s conference and also an invitation to other events and seminars on the security issue.
www.icsss.eu/en/

Štěpán Kavan
editor

THE ROLE OF TRANSNATIONAL AND SUBREGIONAL CRISIS MANAGEMENT IN CRISIS MANAGEMENT

Radka RYPL DUŠKOVÁ

Brno, Czech Republic

https://doi.org/10.36682/SSS_2024_1

ABSTRACT: The article focuses on the analysis of the role of transnational and subregional crisis management in the field of security in crisis management. With the increasing threats such as natural disasters, terrorism, pandemics, and military conflicts, it is essential to coordinate the activities of security forces at both regional and international levels. The paper examines the structure and functioning of crisis management within transnational organizations (eg, the EU, the UN) and subregional collaborations, which play a key role in preventing and addressing crises. It also explores the coordination between individual member states, their crisis teams, and other actors, such as non-governmental organizations and the private sector. The conclusion discusses the effectiveness of these collaborations and offers recommendations for improving crisis management in the field of security in the context of global and regional challenges.

KEY WORDS: Crisis Management; Emergency Management, Common Foreign and Security Policy.

INTRODUCTION

Crisis management is currently experiencing turbulent times at all levels of governance around the world on all continents. Governments have to respond to growing economic problems, military challenges, issues of civilian emergency planning, as well as foreign policy changes that negatively affect the stability of many previously very stable sectors (Kurilovska, Mullerova, 2023).

A crisis is a challenging and pivotal moment with the potential to cause disruption and destruction. Crisis management is essential to minimize potential damage and aid in faster recovery. Understanding the definition and history of crises and crisis management is essential for effective crisis management (Sawang, 2023).

Since the beginning of 2020, the world has been changing on a scale and with an intensity that no one could have predicted. The year 2022 has shown that in addition to dealing with Covid-19, we will be dealing with another long-term crisis caused by the war in Ukraine, which will have ongoing and more serious consequences in the future. These two major crises are accompanied by the most serious and boundless climate change, which has increasingly strong negative effects of various kinds, such as heat waves, drought, erosion or floods. All of these global crises have an impact on society and politics, we perceive disruptions in the field of established businesses, entrepreneurship, but also in the field of innovation and global management (Bouncken, Kraus, De Lucas Ancillo, 2022).

Climate change, including increases in greenhouse gas concentrations in the atmosphere, increases in air and ocean temperatures, melting glaciers and rising sea levels, are risk multipliers. These problems then even threaten the peace and security of humanity due to conflicts arising at national, regional and international levels. Strategic management of the

climate crisis and its risk to the coastal zone is therefore vital to the health and well-being of the global biogeosphere (Nugawela, Mahaliyana, Abhiram, 2023).

CRISIS MANAGEMENT IN THE EU

Since its foundation and throughout the formal and informal dimensions of its integration process, the European Union (EU) has always been confronted with questions of peace and violence, not only internally but also externally. However, the specific context of the emergence of the Common Foreign and Security Policy (CFSP)/European Security and Defense Policy (ESDP) was characterized by evolving security threats that included terrorism, failed states and violent internal conflicts, which required a different approach in terms of the EU's ability to respond to crises and violence inside and outside its borders. In addition, the EU also has the difficult task of seeking consensus among its member states as to why, where and how to deploy peacekeeping missions, responding both to domestic political and economic dynamics and to the overall institutional goal of promoting security within and beyond the EU (Freire, Lopes, Nascimento, 2015).

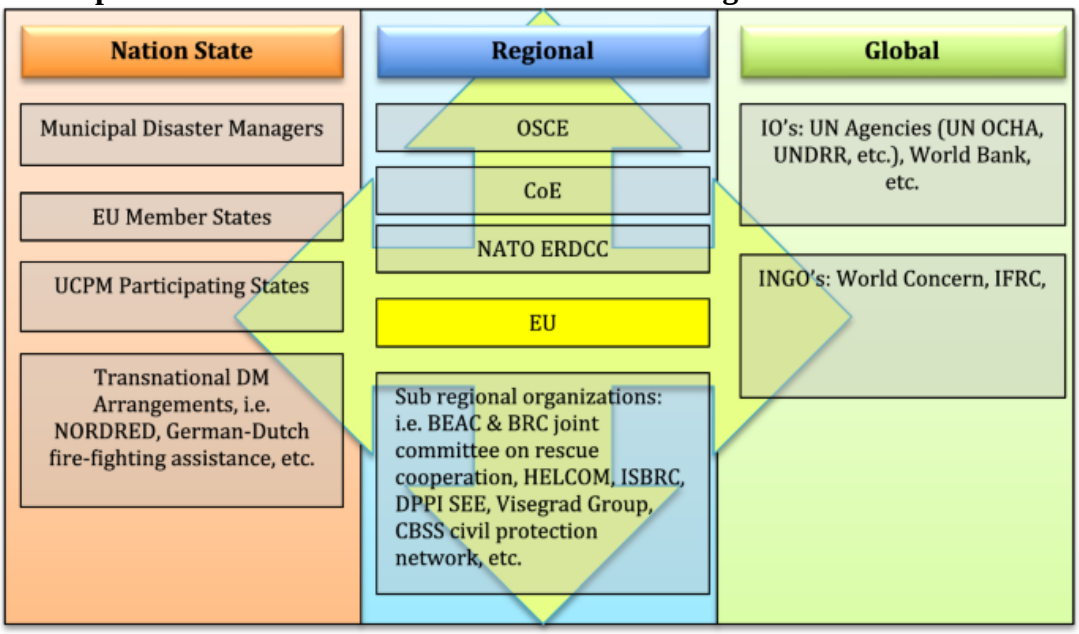
Due to the regional decline of state power, difficulties in maintaining order in some countries would increase regional instability and the likelihood of terrorist attacks on European soil. Crisis management in the Common Foreign and Security Policy (CFSP) has a similar structure to the general models, albeit adapted to the nature of the EU's objectives. So far, the EU has focused international efforts in crisis management on prevention. In this way, the foreign policy dimension of European crisis management expands beyond the strict boundaries of the rule of law: economic and social development is the pillar of a solid and contemporary nation (Galluccio, 2021).

Through the Union Civil Protection Mechanism (UCPM), the EU now has the ability not only to facilitate but also to provide capacities to Member States in the event of cross-border disasters, such as air support for forest fires, urban rescue search teams and emergency medical teams. Of course, the existence and potential increase in the intensity and number of transboundary disasters remains a strong argument for why states choose to cooperate in disaster mitigation and response. The practice of disaster management, even if managed with respect to existing legal conditions of cooperation, also opens up possibilities for further integration through collective recognition of improved crisis coordination (Hollis, 2020).

European crisis responses involve complex layers of diverse actors from different sectors and levels of government coming together momentarily under extreme time demands to jointly coordinate responses to cross-border crises. This can include various informal governmental and non-governmental networks and actors, from the Euro-Atlantic Disaster Response Coordination Center (EADRCC) to public-private cooperation in logistics (Hollis, 2020).

The complex interaction between levels of crisis management is illustrated in Figure 1. Some of the main organizations and measures used to mitigate or respond to cross-border crises in Europe are listed here. The figure only provides a general overview of European crisis coordination, where the four-pointed arrow in the background of the figure indicates a complex set of interactions that link some but not all crisis management measures (Hollis, 2020).

Fig. 1: Complex interactions between levels of crisis management in the EU



Source: Hollis, 2020.

The importance of transnational and sub-regional crisis management in Europe is also highlighted by the complex selection of interactions between government officials, private companies, NGOs and international organizations (Hollis, 2020).

The importance of transnational and subregional crisis management lies in its ability to effectively coordinate and manage responses to crisis situations that cross the borders of individual states or that have a significant impact on specific geographic areas. This type of crisis management is becoming increasingly important due to the increasing complexity and scale of global threats such as natural disasters, pandemics, terrorism or geopolitical conflicts.

- Transnational crisis management involves coordination between different states through international organizations such as the European Union, the United Nations, or the World Health Organization. This type of cooperation is key to managing crises that require a rapid and coordinated response, such as pandemics, climate change or terrorist attacks. Transnational organizations can provide the necessary resources, expertise and coordination beyond the capabilities of individual states.
- Subregional crisis management focuses on cooperation between states within a certain geographical area, for example within Central Europe, the Balkans or Africa. This model is particularly important for solving crises that affect specific regions, such as natural disasters (eg floods or earthquakes), migration, political instability or economic crises. Subregional cooperation often includes information exchange, joint crisis plans, exercises and training, enabling better preparation and effective response to emerging threats.

Transnational and sub-regional crisis management plays a key role in the field of security, as it enables coordination between different actors (governments, non-profit organizations, militaries and the private sector), leading to a faster and more effective response to crisis situations. Without such coordination, individual states could face greater challenges in protecting their citizens and infrastructure. The importance of this approach grows especially in connection with global challenges that cannot be effectively solved only at the national level. This method of crisis management provides a framework for effective sharing of resources, ensuring continuity of operations and protection, and supporting recovery after crisis events,

which strengthens security not only at the national, but also at the international and regional levels.

METHODOLOGY AND OBJECTIVE

The review of available literature in the field is carried out scientifically and systematically (Kraus, Breier, Lim, et al., 2022). A combination of qualitative research and comparative analysis was chosen to analyze the role of transnational and subregional crisis management in the field of crisis management. This methodology makes it possible to examine in detail the functioning and effectiveness of various crisis structures within transnational organizations and subregional cooperation.

Selection of case studies – specific cases of crisis management were selected to illustrate cooperation at the transnational and subregional level. Cases analyzed include:

- **European Union (EU)**: Managing migration during the refugee crisis (2015–2016) and the response to the COVID-19 pandemic.
- **United Nations (UN)**: UN involvement in natural disaster management, such as the 2010 Haiti earthquake.
- **Subregional cooperation in Europe**: The Visegrad Four and its role in addressing regional security challenges.

The case studies were chosen based on their relevance to the investigated aspects of crisis management, such as coordination between actors and the effectiveness of the measures taken.

Data Collection - Data was obtained from several sources:

- **Primary sources**: Documents and reports of transnational organizations (EU, UN) and subregional initiatives.
- **Secondary sources**: Academic literature, professional articles and publications focused on crisis management.

Analytical methods:

- **Comparative analysis**: Comparison of crisis management structures and mechanisms between individual transnational and subregional entities.
- **Content analysis**: Analysis of documents and reports to identify key factors affecting the effectiveness of crisis management.
- **Thematic analysis**: Identification of common themes and challenges in the field of coordination and cooperation between actors.

Limitations of the research – the methodology was limited by the availability of data from internal sources of crisis management. Another limitation was the diversity of structures and legal frameworks of individual organizations, which makes their direct comparison difficult. These factors were taken into account when interpreting the results.

Results – The described methodological approaches enable a comprehensive evaluation of the role of transnational and subregional crisis management in the context of current challenges. The knowledge gained contributes to the formulation of recommendations for improving crisis management at all levels.

RESULTS AND DISCUSSION

Global crises are complex, especially when it comes to the negative effects they bring with them over time. Usually, the bigger the crisis, the more complex its effects and the more difficult it is to find ways out of the crisis. Understanding crisis as a process requires crisis

managers to strategize and act to identify ways to get out of ongoing crises (Bouncken, Kraus, De Lucas Ancillo, 2022).

The last two decades have been characterized by the continuity of various crisis situations. The peace and security crisis that erupts with the Russian invasion of Ukraine in 2022 follows a series of other global crises, such as the large-scale security crisis following the attacks of September 11, 2001, the financial crisis of the end of the 21st century, the migration "crisis" of 2015-2016 and the health crisis caused by the Covid-19 pandemic in 2020 and beyond. Along with some persistent long-term challenges such as the climate crisis, it seems legitimate to argue that the state – or narrative – of crisis is in many ways a normality that defines the context in which different levels of global, national and local governance operate. (Heikkilä, Mustaniemi-Laakso, 2023).

States are increasingly confronted with complex choices that require balancing the protection of individual rights with the general interests of society and finding new measures for the distribution of rights and protection in situations where access and availability of resources are affected. In acute situations, such decisions are taken under considerable pressure and often without knowledge of all the circumstances relevant to the decision (Marique 2020, P. 63; Heikkilä, Mustaniemi-Laakso, 2023).

Time constraints and resource limits require redoubled efforts to conceptualize, create and implement new ideas, goods and services with innovative thinking (Sharma, Kraus, Srivastava, Chopra, Kallmuenzer, 2022). Examples include counter-terrorism measures and preparedness, which play a critical role in security planning and in addressing mass gatherings, soft targets and critical infrastructure in urban environments. (González-Villa, et al., 2023).

In the context of globalized and complex crisis situations that exceed national borders or have a specific regional character, transnational and subregional crisis management plays an irreplaceable role in modern crisis management. This level of governance is necessary for several key reasons that are essential to an effective and coordinated response to crises:

1. Crossing national borders in crisis situations

Many crises, such as natural disasters, pandemics, terrorist attacks, migration or war conflicts, have a scale that goes far beyond national borders. When a crisis affects multiple countries or regions, it is necessary to have mechanisms in place to enable effective coordination between these states and organizations.

- **Examples:** Natural disasters such as hurricanes or tsunamis can hit several countries at once, pandemics (such as Covid-19) spread across countries, and international terrorism often knows no borders. Transnational organizations such as the UN, WHO or the EU are essential for effective coordination and resource mobilization between states.

2. Ensuring coordination and cooperation between states

In crisis situations, it is important that the affected states work together to solve the problem together. Without effective coordination, there can be duplication of measures, chaos, or, on the contrary, a lack of help where it is most needed. Transnational and subregional crisis management facilitates the coordination and unification of various national, regional and international components of crisis management.

- **Examples:** In the case of humanitarian disasters, such as the conflict in Syria, organizations such as the European Union or NATO can coordinate aid, the deployment of military or humanitarian forces, and diplomacy between different countries.

3. Rapid mobilization of resources and professional assistance

Crisis situations often require the rapid mobilization of resources and experts, which individual states cannot provide in sufficient quantities on their own. Transnational and subregional crisis management enables the rapid and efficient distribution of financial aid, material, medical aid and other supplies to affected areas.

- **Examples:** In response to natural disasters, such as the tsunami in 2004 or the earthquake in Haiti, immediate assistance was needed from various states and organizations. Transnational and subregional organizations can pool resources, coordinate logistics, and ensure rapid response.

4. Prevention and mitigation of global threats

Many crises, such as pandemics, cyber-attacks, climate change or organized crime, are global in nature, meaning that their effects can be significantly large-scale, affecting multiple countries or entire regions. Without international cooperation, it would be very difficult to effectively counter these threats.

- **Examples:** Global warming and its effects on the environment call for coordinated policies between states and at the supranational level (for example, within the framework of the Paris Climate Agreement), as well as in the case of global health crises, where coordination between the WHO, national governments and international organizations can decide success in preventing the spread of disease.

5. Ensuring security and stabilization in crisis areas

In crisis situations, especially in or after armed conflict, stabilizing the situation and ensuring security can be key to restoring order. Multinational organizations such as the UN, NATO or the EU have the ability to deploy military, police and civilian forces that can help stabilize the situation and restore the rule of law.

- **Examples:** UN military missions in conflict zones (for example in Sudan or the Balkans) are an example of the use of transnational crisis management to restore stability and ensure peace.

6. Support of vulnerable and affected areas

In crisis situations, it often turns out that some areas or communities are particularly vulnerable and require specific assistance that can only be provided by transnational and subregional mechanisms. It can be help in the case of migration, providing protection for refugees or humanitarian aid for affected areas.

- **Examples:** In the case of migration, which occurs most often as a result of armed conflicts or natural disasters, transnational organizations such as the Office of the United Nations High Commissioner for Refugees (UNHCR) provide coordination between states and assistance to refugees.

7. Resolution of regional conflicts and crises

Subregional crisis management focuses on specific regional threats and allows countries in a given region to work together and respond to issues that relate to their specific geopolitical context. Regional organizations can provide more effective, targeted and culturally appropriate problem solving than multinational organizations.

- **Examples:** In Africa, the African Union (AU) is a key sub-regional player coordinating peacekeeping operations and crisis responses within the continent, while the Association of Southeast Asian Nations (ASEAN) focuses on crisis management in Southeast Asia.

8. Ensuring a comprehensive response and integrated strategy

Crises that are characterized by their complexity require a multidimensional approach to their solution. Transnational and subregional crisis management enables an integrated approach that includes military, humanitarian, health, economic and environmental aspects.

- **Examples:** In complex crises, such as migration waves, which have economic, political and humanitarian dimensions, transnational and subregional management allows for the coordination of all these aspects into one overall strategy.

Transnational and subregional crisis management are key tools for the effective resolution of crises that cross national borders or have a specific regional character. However, despite their

importance, their application presents a number of problems and challenges that can hinder effective crisis management. These problems are linked to political, organizational, legal and logistical factors that can affect the ability of these mechanisms to manage crisis situations. The main problems include the following:

1. Political and diplomatic obstacles

One of the most significant problems of transnational and subregional crisis management is political and diplomatic differences between member states. Each state has its own national interests, political priorities and strategic goals, which may not always agree with the overall goals of crisis management at the international or subregional level.

- **National sovereignty**: Some states may be reluctant to accept interventions by supranational organizations or subregional partners in their internal crisis management, which may lead to inconsistencies in crisis response.
- **Different priorities**: Each state may have different priorities in crisis management, which can slow down or block decision-making and coordination among the actors involved.
- **Lack of political will**: There can sometimes be a lack of willingness to cooperate at the state level, which can lead to ineffective crisis management and delayed responses to crisis situations.

2. Communication and coordination

Effective communication and coordination between the various actors involved (government bodies, international organizations, humanitarian organizations, military units, local communities, etc.) is essential for successful crisis management. However, problems in these areas can greatly complicate effective responses to crisis situations.

- **Lack of shared infrastructure and data**: Different organizations may have different systems for collecting and sharing information, which can lead to incomplete or delayed information.
- **Language, cultural and religious barriers**: If the crisis involves different linguistic, cultural and religious backgrounds, this can slow down communication between the parties involved.
- **Coordination problems**: In crisis situations, there may be overlapping responsibilities between different entities, leading to duplication of efforts or, conversely, gaps in the response to crisis events.

3. Legal and regulatory issues

Legal frameworks at the international and subregional level are often not sufficiently unified, which can cause problems in the application of crisis management. Legal norms, regulations and competences can differ between states, which can lead to problems in providing assistance or coordinating a response to a crisis situation.

- **Inconsistency in legislation**: Different countries may have different legal norms regarding crisis management, for example in the area of military intervention, protection of human rights or liability for damages caused by crisis measures.
- **Insufficient international legislation**: In some areas, for example in the fight against international terrorism or in the prevention of global health crises, there is a lack of effective international legal frameworks that would facilitate cooperation and exchange of information between states.

4. Financial and material limitations

Crisis situations often require the rapid deployment of extensive resources, including financial resources, material aid and human capacity. However, not only financial, but also material and logistical problems can represent a significant obstacle in effective crisis management.

- **Lack of funds**: International and subregional organizations often face a lack of funds to provide immediate assistance in crisis situations. Time-consuming approval of funds between member states can slow down the response to a crisis.
- **Logistical issues**: Coordinating the delivery of humanitarian aid, securing the necessary equipment and supplies can be difficult, especially in areas that are difficult to access or have insufficient infrastructure.
- **Distribution of resources**: When a crisis situation is large, it can be difficult to distribute aid evenly and efficiently among affected areas, which can lead to uneven coverage of needs.

5. Different levels of preparedness and capacity between states

Different states have different capacities and levels of preparedness for crisis situations, which can affect the ability of transnational and subregional crisis management to function effectively.

- **Uneven preparedness**: Some states, especially those with limited economic and logistical resources, may not have sufficiently developed crisis plans, experts, or infrastructure for effective crisis management.
- **Dependence on external aid**: Some states may be heavily dependent on aid from multinational organizations or wealthier states, which can slow down and make effective responses in crisis situations difficult.

6. Security and military challenges

In crisis situations, especially when it comes to armed conflicts or terrorist attacks, it can be difficult to coordinate military and civilian components, which can lead to security issues and conflicts between the parties involved.

- **Insufficient military coordination**: In military operations aimed at ensuring the security and stabilization of a crisis region, it can be difficult to coordinate actions between the military components of different states and international organizations.
- **Insecure areas and the presence of armed groups**: In crisis areas, it can be difficult to provide security for aid workers, military units and other actors, which can slow down the delivery of aid and protect vulnerable groups.

CONCLUSION

Transnational and subregional crisis management are essential tools for the effective management of crisis situations that transcend national borders or are limited to specific regions. These forms of cooperation enable a quick response to threats, optimal use of available resources, and ensuring security and stability on a global and regional level. Given the increasing challenges that characterize the contemporary world, it is imperative that crisis management continues to strengthen these supranational and subregional mechanisms that will be able to effectively respond to emerging threats and protect both individual states and the global community.

REFERENCES AND INFORMATION SOURCES

1. BOUNCKEN, RB, KRAUS, S., DE LUCAS ANCILLO, A. Management in times of crises: reflections on characteristics, avoiding pitfalls, and pathways out. *Rev Manag Sci* 16, 2035–2046 (2022). https://doi.org/10.1007/s11846-022-00580-2.
2. FREIRE, MR, LOPES, PD, NASCIMENTO, D. (2015). The EU's Role in Crisis Management: The Case of the EUMM. In *Palgrave Macmillan UK eBooks* (pp. 178–195). https://doi.org/10.1057/9781137442253_9.

3. GALLUCCIO, M. (2021). Crisis Management and Risk Assessment in the EU: A General Outline. In *Springer eBooks* (pp. 103–109). https://doi.org/10.1007/978-3-030-60414-1_9.
4. GONZÁLEZ-VILLA, J. *et al.* (2023). Decision-Support System for Safety and Security Assessment and Management in Smart Cities. *Multimedia Tools and Applications*, *83* (22), 61971–61994. https://doi.org/10.1007/s11042-023-16020-6.
5. HEIKKILÄ, M., MUSTANIEMI-LAAKSO, M. (2023). Introduction: Approaches to Vulnerability in Times of Crisis. *Human Rights Review*, *24* (2), 151–170. https://doi.org/10.1007/s12142-023-00694-4.
6. HOLLIS, S. Crisis management in Europe: exploring transgovernmental solutions to transboundary problems. *J Transatl Stud* 18, 231–252 (2020). https://doi.org/10.1057/s42738-020-00042-1.
7. KRAUS, S., BREIER, M., LIM, WM *et al.* Literature reviews as independent studies: guidelines for academic practice. *Rev Manag Sci* 16, 2577–2595 (2022). https://doi.org/10.1007/s11846-022-00588-8.
8. KURILOVSKA, L., MULLEROVA, J. (2023). Analysis of Crisis Management Systems in the Context of the Global Economic Crisis and Military-Political Changes. In: Cayón Peña, J., Ramírez, JM (eds) Threats to Peace and International Security: Asia versus the West. *Advanced Sciences and Technologies for Security Applications* (pp. 205–228). Springer, Cham. https://doi.org/10.1007/978-3-031-28336-9_11.
9. MARIQUE, Y. (2020). A "New Normal": Legality in Times of Necessity: French Administrative Law under the Health Emergency. In *University of Essex eBooks*. http://repository.essex.ac.uk/28023/.
10. NUGAWELA, NPPS, MAHALIYANA, AS, ABHIRAM, G. (2023). Climate Crisis and Coastal Risk Management. In: Chatterjee, U., Shaw, R., Kumar, S., Raj, AD, Das, S. (eds) Climate Crisis: Adaptive Approaches and Sustainability. *Sustainable Development Goals Series*. Springer, Cham. https://doi.org/10.1007/978-3-031-44397-8_29.
11. SAWANG, S. (2023). Understanding crisis management in modern societies. In *Springer eBooks* (pp. 1–16). https://doi.org/10.1007/978-3-031-25188-7_1.
12. SHARMA, GD, KRAUS, S., SRIVASTAVA, M., CHOPRA, R., KALLMUENZER, A. (2022). The changing role of innovation for crisis management in times of COVID-19: An integrative literature review. *Journal of Innovation & Knowledge*, *7* (4), 100281. https://doi.org/10.1016/j.jik.2022.100281.

CONTACT INFORMATION

PhDr. Radka RYPL DUŠKOVÁ
Department of Military Theory
Faculty of Military Leadership
Defense University
Kounicova 65, 662 10 Brno
Czech Republic
radka.ryplduskova@unob.cz
ORCID ID – 0009-0008-9310-8892

CONSPIRACY THEORIES AND HOAXES AS PART OF HYBRID THREATS AND THEIR NEGATIVE IMPACT ON SECURITY OF SOCIETY[1]

Radoslav IVANČÍK

Police Academy in Bratislava, Slovak Republic

https://doi.org/10.36682/SSS_2024_2

ABSTRACT: Conspiracy theories and hoaxes exist in all societies. Their influence and popularity have been constantly increasing in recent years, especially in close connection with the rapid increase in the use of modern information and communication technologies, systems and devices, with the emergence of new media and especially the mass use of social networks. Some conspiracy theories and hoaxes can be just harmless fun or a manifestation of a certain disbelief, skepticism or recession. However, some of them can be very dangerous because they can be part of hybrid threats spread by state and/or non-state actors with the aim of influencing the opinion, behavior and reactions of the population in the target countries with the aim of disrupting the functioning of a democratic society, questioning democratic principles, endangering democratic processes, undermining trust in democratic institutions and democratically elected representatives and in the ability to solve current problems of society. Some may even lead to xenophobia and populism, to the promotion of violence, extremism, radicalism and ethnic, racial or religious intolerance. This is also why today conspiracy theories and hoaxes represent a threat and at the same time a challenge for human, especially democratic society, and this is also why the author of this paper deals with them as part of his interdisciplinary scientific research.

KEYWORDS: Conspiracy theories, hoaxes, hybrid threats, democratic society.

INTRODUCTION

The current modern human civilization is significantly influenced by deepening globalization processes, which manifest themselves to a greater or lesser extent in all spheres of society's life. With one of the manifestations of the current modern era, closely connected with the growing computerization, internetization and digitalization of society, the dynamic emergence of new media and the rapid development and increasingly massive use of sophisticated information and communication technologies, systems and means, a new range of possibilities has also appeared, such as all kinds of news, rumours, news or theories not only to search for and receive, but also to create or modify and then further share and spread. At the same time, however, a new range of possibilities has also appeared, such as abusing modern technologies, devices, media and especially social networks (Kuchtová, 2018; Hajdúková, 2022) and spreading through them invented, altered, distorted, deceptive and misleading information in the form of various conspiracy theories and hoaxes in order to influence people's thinking and actions (Ivančík, 2022). The spread of some conspiracy theories and hoaxes, which react to various significant events, phenomena or processes taking place

[1] "This work was supported by the Research and Development Support Agency on the basis of Contract no. APVV-20-0334."

around us, thus represents a threat that can have very negative, unfavorable consequences for the safety of individuals, social groups and the entire human society.

Some conspiracy theories and hoaxes can be just harmless fun, a joke, or a manifestation of a recession based on an anti-conventional attitude within society, or a manifestation of a certain mistrust, skepticism or doubt about the official explanations of some politically, economically, socially, militarily or otherwise significant events, phenomena or processes (for example, economic, financial, energy crises, wars, conflicts, epidemics, pandemics, climate changes, tragic events, deaths of prominent personalities, etc.).

However, some conspiracy theories and hoaxes can be very dangerous, as they can be part of hybrid threats spread by state and/or non-state actors with the primary goal of influencing the thinking, opinion, actions and behavior of the population and at the same time creating chaos, uncertainty, polarizing and destabilizing society, disrupting its normal functioning, undermine the authority and trust in democratic institutions, democratically elected representatives, democratic rules, principles and principles and also in the ability to solve current societal problems in target countries. At the same time, they can lead to the promotion of violence, xenophobia, extremism, radicalism or ethnic, racial or religious intolerance. This is also why some conspiracy theories and hoaxes currently represent a very serious threat and at the same time a challenge especially for democratic societies (Ivančík, 2022).

1 CONSPIRACY THEORIES AND HOAXES AS PART OF HYBRID THREATS

Some conspiracy theories and hoaxes can be considered as forms of hybrid threats precisely for the above reasons. Their dissemination is by no means just harmless fun, a joke, or an expression of certain skepticism on the part of some individuals about the official explanations of some significant events, but represents a carefully thought-out move, the only real intention of which is to promote predetermined strategic political and ideological goals. These are not just "ordinary conspiracy theories", such as those about aliens who live among us because their spaceship crashed here and they can't get home, so they took the form of people and adapted to the conditions of life on Earth (Greigová, 2019) , or just "ordinary hoaxes" in the form of various false alarm messages that warn of non-existent dangerous viruses, or false pleas for help or petitions that contain calls for their further dissemination (Nutil, 2018).

In this case, as mentioned above, it is about deliberate, purposefully edited half-truths or a whole mixture of half-truths, lies and false theories, reports and/or information in the form of conspiracy theories or hoaxes spread by state and/or non-state actors for the purpose of support in achieving advance set strategic political and ideological (in certain cases also economic and other) goals based on individual methods and procedures used in the spread of hybrid threats in the conduct of hybrid warfare. It is a conscious and deliberate activity aimed at manipulating the general public through the dissemination of various fabrications, lies, lies, half-truths, misleading, distorted videos, images and/or stories in order to achieve stated goals.

Based on the above information, this type of conspiracy theories and hoaxes can be said to be a form of political propaganda because they aim to promote political and/or ideological goals. They use a proven strategy for this - they offer attractive explanations of significant political and social events, phenomena and processes, which, although untrue, objectively improbable, focus people's attention in the desired direction. However, individual actors pursue their own interests and goals by spreading such conspiracy theories and hoaxes (Qassam, 2019).

Some conspiracy theories can be considered part of hybrid threats because they are part of non-military, unconventional and asymmetric combat methods and part of conducted information, psychological and intelligence operations aimed at influencing the opinion, thinking and behavior of the population in the target countries and reducing the resistance of the given society. In terms of definition, hybrid threats can be characterized as a set of coercive and subversive activities, conventional and unconventional, military and non-military methods

and tools, used systematically to achieve specific goals without a formal declaration of war and under the pretext of a standard response. They are applied by activities characterized by centrally controlled intelligence and information operations, operations by non-state actors, including paramilitary groups, or the deployment of the armed forces of a state actor without designation. Such activities can begin before openly declared military operations (Lukáčová, 2020, p. 103).

Another definition says that hybrid threats are coordinated and synchronized actions that purposefully target the systemic vulnerability of democratic states and institutions through a wide variety of means, for example activities that use detection and attribution thresholds, as well as different interfaces (war-peace, domestic- external security, local - state and national - international), as well as activities aimed at influencing various forms of decision-making at the local (regional) level, state or institutional level and designed to support and/or fulfill the actor's strategic goals while undermining and/or damaging the goal (Hybrid CoE , 2023).

For a better understanding of the investigated issue and to create a comprehensive picture of why some conspiracy theories and hoaxes can be considered part of hybrid threats, it is necessary - within the framework of the theoretical-methodological starting points of the investigation of the issue in question - to also mention other closely related concepts, such as hybrid influence, hybrid activity (action) and above all hybrid war.

Hybrid influencing is an act, the results of which the instigator achieves through a number of mutually complementary methods and through the use of the vulnerabilities of the target company. Hybrid influence is implemented using and through economic, political or military and other tools. It can also be carried out using information and communication technologies and social networks, while the given methods can be used simultaneously or sequentially (YT, 2017, p. 95).

A hybrid activity (action) is an activity characterized by ambiguity, which arises from the combination of the use of conventional and unconventional means - disinformation, fake news, interference in political debate or elections, disruption of functionality or attacks on critical infrastructure, implementation of information and cyber operations, various forms of criminal activities and asymmetric use of military means and warfare (Zandee et al., 2021, p. 8).

Hybrid war can be understood as a wide range of hostile activities, in which the role of the military component is rather small, because political, informational, economic and psychological influence becomes the main means of conducting the battle. Such methods help to achieve significant results: territorial, political and economic losses of the enemy, chaos and disruption of the system of exercising state power, and the weakening of society's morale (Manko - Mikhiiev, 2018, p. 13). Hybrid warfare can also be characterized as a set of lethal and non-lethal means that a state or non-state actor uses to advance its interests against the will of another actor. At the same time, hybrid war combines several ways of waging war: classic military operations, operations in cyberspace or cyber attacks, espionage, spreading false information with the aim of influencing the enemy's public opinion, etc. (Danyk et al., 2017, p. 6).

2 THE SPREAD AND PERCEPTION OF CONSPIRACY THEORIES AND HOAXES AS PART OF HYBRID THREATS

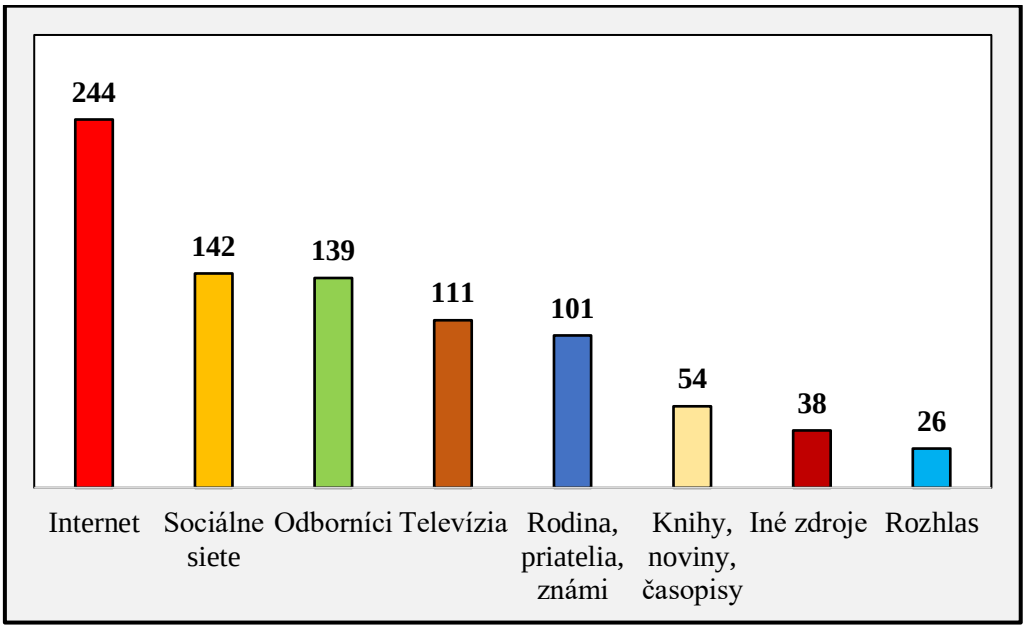
The use of various fabrications, lies, lies, half-truths or twisting of facts in order to influence individuals or even the entire public within the framework of hybrid activities, as already mentioned above, is nothing new, but if it is combined with sophisticated means, such as today's modern "smart devices, means and technologies, with the environment of social networks and the Internet, or the activity of hackers, there is a new and very strong threat of the spread of various types of conspiracy theories, misinformation or hoaxes or so-called fake news

, which represent a danger not only for individuals, social groups and organizations, but in some cases a security threat for the entire contemporary democratic society.

The emergence and rapid development of the Internet and social networks has led to a radical change in the ways in which people today communicate and obtain information. This new way of communication is characterized by the very high speed with which information is transmitted. Social networks offer the highest degree of interaction that current means of communication can provide to users. Access to all kinds of information on the Internet and social networks is almost unlimited and, compared to other options, very cheap, mostly completely free. Also, the lack of effective and efficient measures aimed at regulating online content, in contrast to that which is broadcast (provided, published) through traditional media, makes the online environment of the Internet and social networks extremely interesting and tolerant.

Research carried out at the Academy of the Police Force in Bratislava in 2023, in which 266 students of internal, external and conversion bachelor's, master's and doctoral studies took part, confirmed that the Internet and social networks are the two most used options for obtaining information. They are followed by experts, television, family, friends, acquaintances, the press, books, magazines, newspapers, radio or other sources of information (chart 1).

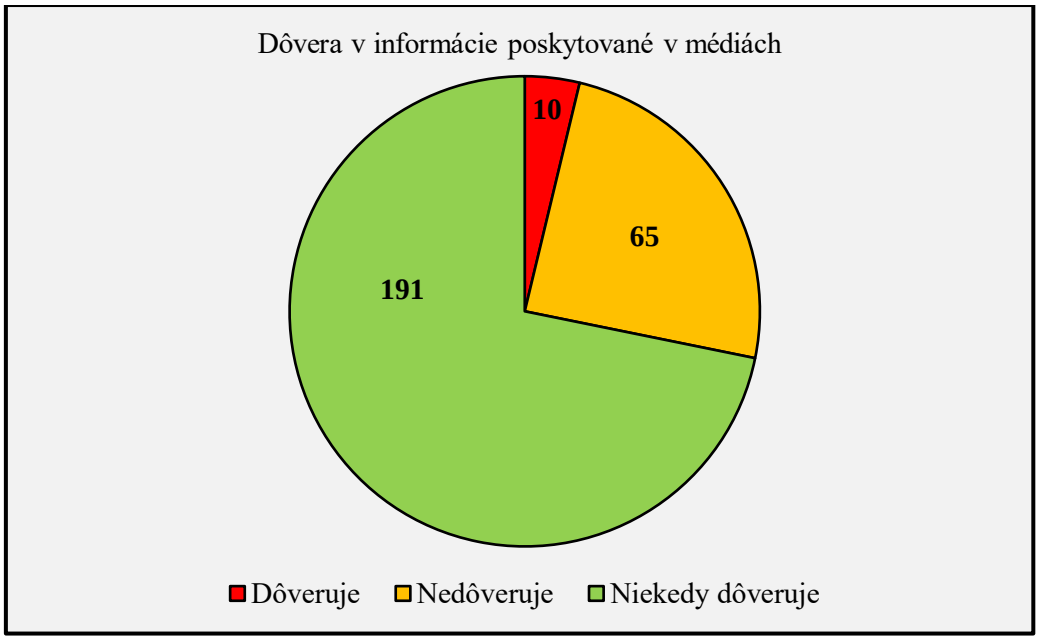
Chart 1: Overview of options used by students in obtaining information (number of students)



Source: Own research

An explanation of why students use the Internet and social networks much more often than traditional media (television, radio, books, magazines, newspapers) to obtain information is offered by the following graph, which shows that only 10 fully trust information from the media (3.76%) students compared to 65 (24.44%) who clearly do not trust the information provided in the media. The largest part of students, as many as 191 (71.80%) trust information obtained from the media only sometimes (chart 2).

Graph 2: Overview of students' trust in the information provided in the media (number of students)

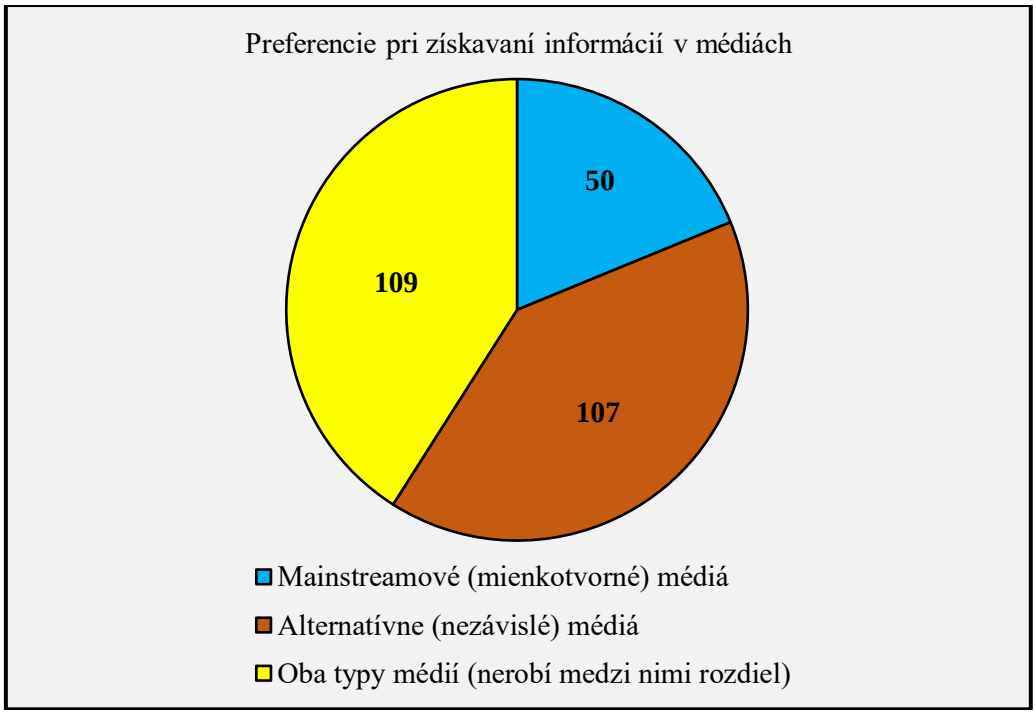


Source: Own research

Due to the low trust of students in the information provided by the media, the research team was interested in this context, whether students - if they do use information from the media - prefer mainstream (opinion-forming) media when obtaining information, or whether they prefer to obtain information from alternative (independent) media. media (portals, sources). The respondents' answers show that the largest part of students - more than four tenths of them (40.98%) - do not differentiate between media when obtaining information, a slightly smaller part of students (40.22%) prefer to use alternative (independent) media and the smallest part of them – less than one fifth (18.80%) – prefer mainstream (opinion-forming) media (graph 3).

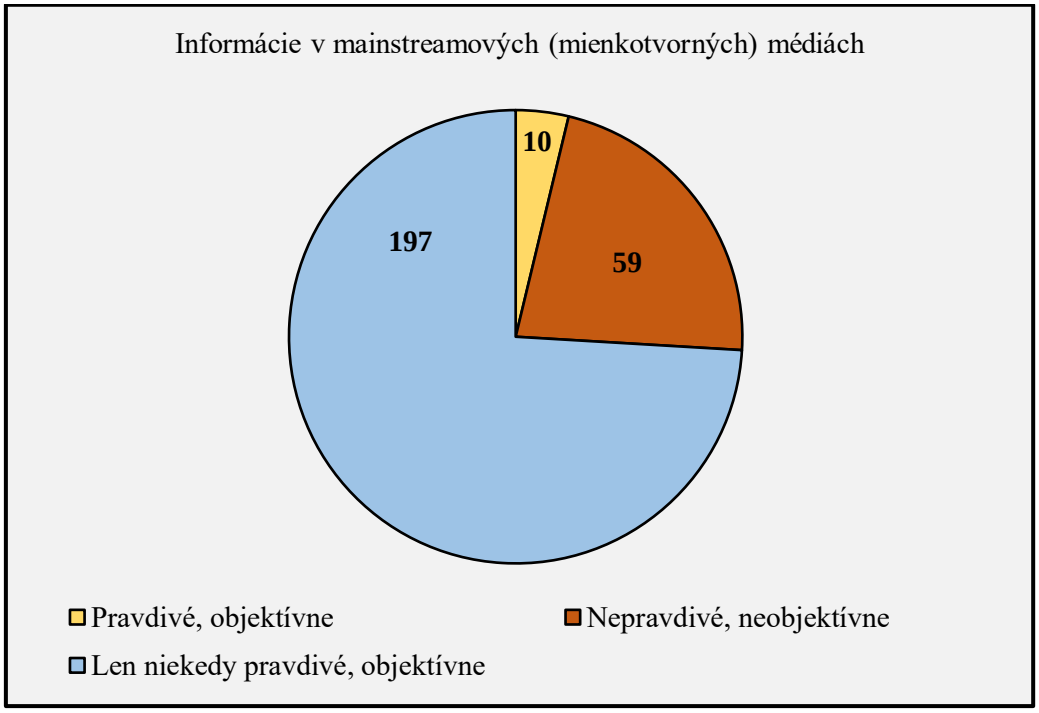
Higher trust of students in alternative (independent) media compared to mainstream (opinion-forming) media is also confirmed by the following answers to the question, which we asked whether they consider the information presented in both types of media to be true, or objectively. It follows from the answers of the respondents that only 10 students (3.76%) consider the information presented in the mainstream (opinion-forming) media to be true, or objectively. In contrast, up to 59 students (22.18%) consider the information published in these media to be false, or biased. The largest part of respondents (74.06%) stated that they consider the information published in the mainstream (opinion-forming) media to be true, or objectively only sometimes (graph 4).

Chart 3: Overview of students' preferences for obtaining information in the media (number of students)



Source: Own research

Graph 4: Overview of students' opinions on truthfulness, or objectivity of information presented in mainstream (opinion-forming) media (number of students)



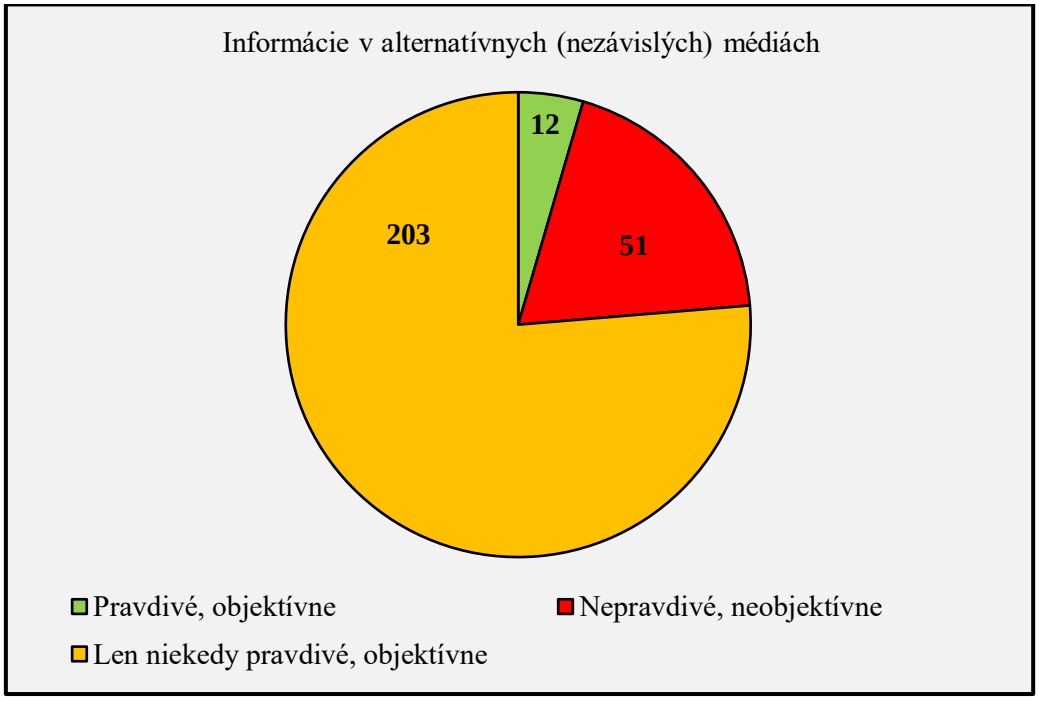
Source: Own research

The slightly higher trust of students in alternative (independent) media compared to mainstream (opinion-forming) media is confirmed by the following answers. It follows from them that 12 students (4.51%) consider the information presented in alternative (independent) media to be true, or objectively. In contrast, up to 51 students (19.17%) consider the information published in these media to be false, or biased. The largest part of respondents (76.32%) stated that they consider the information published in alternative (independent) media to be true, or objectively only sometimes (graph 5).

Although students expressed higher trust in the truth and objectivity of information presented in alternative (independent) media than in mainstream (opinion-forming) media, in general, it can be concluded that trust in the truth and objectivity of information in both types of media is relatively low, and the largest group of students consists of those who who consider the information presented in both types of media to be true and objective only sometimes.

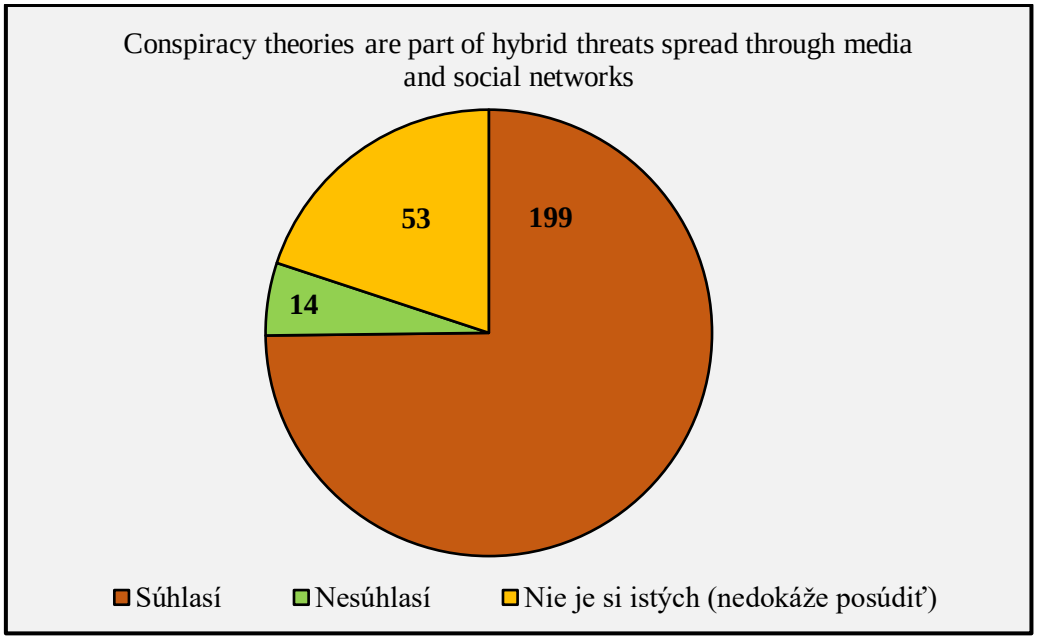
These results are very closely related to the opinions expressed by students when asked if they consider conspiracy theories to be part of the hybrid threats that are disseminated through the media and social networks in the context of hybrid warfare. It follows from the answers of student respondents that almost three quarters of them (74.82%) identify with this opinion. Only roughly one- twentieth of students (5.26%) disagree with it, and one-fifth (19.92%) are not completely sure, or cannot assess it (graph 6).

Chart 5: Overview of students' opinions on truthfulness, or objectivity of information presented in alternative (independent) media (number of students)



Source: Own research

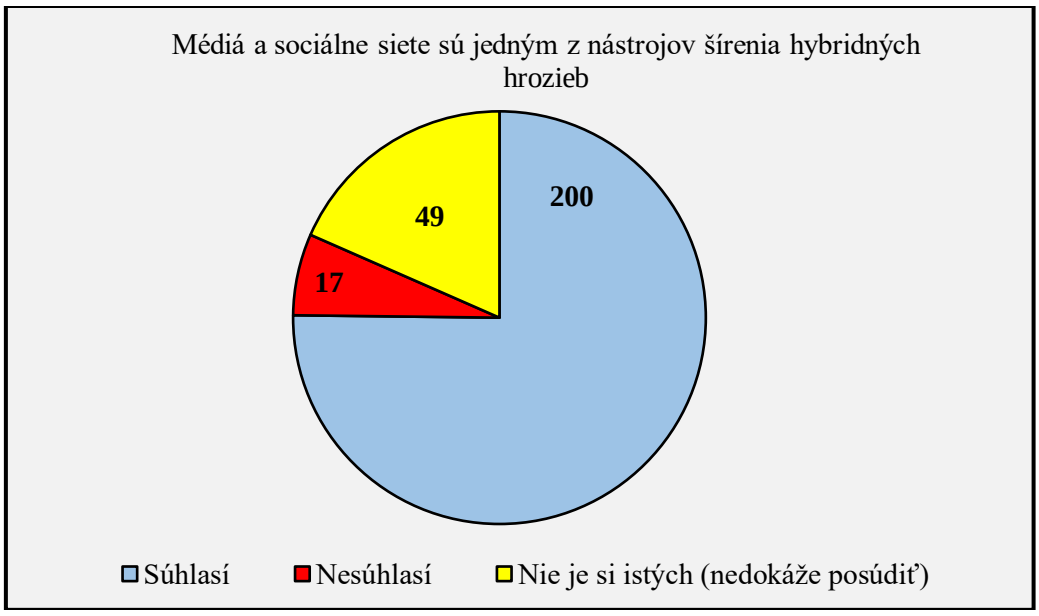
Chart 6: Overview of students' opinions on whether conspiracy theories are part of hybrid threats spread through the media and social networks (number of students)



Source: Own research

Following this, we asked the students whether they consider the media and social networks to be one of the tools for spreading hybrid threats in the context of conducting hybrid warfare. The answers were very similar, as more than three quarters (75.19%) of the student respondents believe that the media and social networks are one of the tools for spreading hybrid threats in the conduct of hybrid warfare. Only 6.19% of respondents do not agree with this opinion, and less than one fifth (18.42%) are not completely sure, or cannot assess it (graph 7).

Graph 7: Overview of students' opinions on whether the media and social networks are one of the tools for spreading hybrid threats (number of students)



Source: Own research

CONCLUSION

In recent decades, also due to the dynamic development of human society, especially in the field of information and communication technologies, systems and means, our way of social functioning has changed significantly. In recent years, the coronavirus pandemic and the measures taken to eliminate its spread and protect public health have played a fundamental role in this change. The progressive internetization, computerization and digitalization of society, as well as the advent of new media and the massive use of social networks, have brought many positives, but also several negatives. These are usually related to anonymity on social networks, distortion of reality or showing unrealistic values that should not even be values. Media, internet and social networks have become a fixed part of our daily life. Among them, especially social networks have become a very powerful communication tool that has changed the way of interpersonal communication.

They really bring a lot of positives, for example, we can talk to a classmate from primary, secondary or university or a friend from childhood whom we haven't seen for many years, find out what interests a person we like, whom we recognize, etc. Social networks also significantly accelerate the flow of information, data, the spread of thoughts and ideas. Among the positive effects, we can also mention various support groups for people who have various health problems or belong to a minority community, help in education or in providing space for education, creativity or self-expression, of course, if they are used correctly.

Unfortunately, social networks and their mass use (and in many cases also abuse) also have their dark sides, and there are quite a few of them. One of them is (among others) the fact that they provide an opportunity to spread various conspiracy theories and hoaxes through them, which can very adversely affect people's thinking, actions, behavior and reactions, disrupt the functioning of society, question existing democratic values, principles and principles, the activities of democratic institutions, the ability to act, solve problems, and thus threaten the entire democratic society. Together with some media, they thus represent one of the tools for spreading hybrid threats within the framework of conducting a hybrid war. The above is also confirmed by the results of research carried out among students of internal, external and conversion studies as part of bachelor's, master's and doctoral studies at the Police Academy in Bratislava.

This is also why it is very important for the state and its competent institutions to take effective and efficient measures to combat hybrid threats, support the acquisition of digital skills, prevention and education in the field of media literacy and working with information. Increasing awareness of conspiracy theories and hoaxes, improving the ability to recognize and detect them, as well as eliminating their spread as much as possible would certainly mean fewer opportunities for, for example, populism, radicalism, extremism, xenophobia or polarization in society. For this reason, the involvement of the state in this issue is not only desirable, but literally necessary. On the other hand, we must all realize that the possibilities of the state are not endless, the state will not solve everything for us, so it is necessary that we ourselves contribute to eliminating the influence of conspiracy theories and hoaxes and their spreaders on our lives.

REFERENCES AND INFORMATION SOURCES

1. BYFORD, J. (2011): *Conspiracy Theories: A Critical Introduction*. London: Palgrave Macmillan, 2011. 179 pp. ISBN 978-0-23027-279-8.
2. DANYK, Y. – MALIARCHUK, T. – BRIGGS, C. (2017): Hybrid War: High-tech, Information and Cyber Conflicts. In *Connections,* 2017, Vol. 16, no. 2, pp. 5-24. ISSN 1812-1098.

3. GREIGOVÁ, C. (2019): *Conspiracy theory*. Brno: CPress, 2019. 128 p. ISBN 978-80-264-2831-2.
4. HAJDÚKOVÁ, T. (2022): Abuse of electronic services for sexual abuse of children. In *Security of electronic communication - a collection of contributions from a scientific conference with international participation*. Bratislava: Police Academy, 2022, p. 71-85. ISBN 978-80-8054-968-8.
5. Hybrid CoE. (2023): Hybrid threats as a concept. In *The European Center of Excellence for Countering Hybrid Threats*, 2023. [online]. [cit. 2024-07-30]. Available from: <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/>.
6. IVANČÍK, R. (2016): Hybrid war – war of the 21st century. In *Almanac – current issues of world economy and politics*, 2016, vol. 11, no. 1, pp. 16-35. ISSN 1339-3502.
7. IVANČÍK, R. (2022): Conspiracy theories – basic theoretical starting points. In *Auspicia*, 2022, vol. 19, no. 1, p. 8-20. ISSN 2464-7217. DOI: 10.36682/a_2022_1_1
8. KUCHTOVÁ, J. (2018): Current trends related to the use of modern technologies. In *Current challenges of cyber security - a collection of contributions from a scientific conference with international participation*. Bratislava: Police Academy, 2018, p. 90-98. ISBN 978-80-8054-773-8.
9. LUKÁČOVÁ, J. (2020): Hybrid threats in the cyber environment. In *Current challenges of cyber security - a collection of contributions from a scientific conference with international participation*. Bratislava: Police Academy in Bratislava, 2020, p. 101-105. ISBN 978-80-8040-819-3.
10. MANKO, O. – MIKHIEIEV, Y. (2018): Defining the Concept of 'Hybrid Warfare ' Based on Analysis of Russian Aggression against Ukraine. In *Information & Security: An International Journal*, 2018, vol. 41, p. 11-20. ISSN 0861-5160.
11. METEŇKO, J. – METEŇKOVÁ, M. (2023): Critical Analysis Criminalistics and Forensic Science Education – at Universities in Slovakia. In *Journal of International Scientific Publications: Educational Alternatives*, 2023, vol. 21, p. 376-389. ISSN 1314-7277.
12. QASSAM, C. (2019): *Conspiracy Theories*. Cambridge: Polity Press, 2019. 140 p. ISBN 978-1-5095-3583-5.
13. USCINSKI, JE – PARENT, JM (2014): *American Conspiracy Theories*. Oxford: Oxford University Press, 2014. 221 p. ISBN 978-0-199-35181-7.
14. YT. (2017): Security Strategy for Society. In *Yhteiskunnan Turvallisuus*, 2017. [online]. [cit. 2024-07-30]. Available from: <https://turvalliskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf>.
15. ZANDEE, D. (2021): Hybrid threats: searching for a definition. In *the Netherlands Institute of International Relations*, 2021. [online]. [cit. 2024-07-30]. Available from: <https://www.clingendael.org/pub/2021/countering-hybrid-threats/2-hybrid-threats-searching-for-a-definition/>.

CONTACT INFORMATION

colonel gst. with doc. Ing. Radoslav IVANČÍK, PhD. et PhD., MBA, MSc.
Police Academy in Bratislava
Sklabinská 1, 935 17 Bratislava
Slovak Republic
radoslav.ivancik@akademiapz.sk
ORCID ID – 0000-0003-2233-1014

ON THE EUROPEAN APPROACH TO COMBATING HYBRID THREATS

Radoslav IVANČÍK

Police Academy in Bratislava, Slovak Republic

https://doi.org/10.36682/SSS_2024_3

ABSTRACT: Hybrid threats in the form of cyber-attacks on public and private computer networks and systems, economic coercion and/or the spread of disinformation and propaganda are becoming more and more frequent and sophisticated. Hybrid attacks can have significant social and economic consequences, including disrupting the functioning of a democratic society, breaching critical infrastructure, stealing intellectual property and/or manipulating financial markets. These threats are designed to be difficult to detect and identify, which makes it difficult for individual states and transnational groups to react. Therefore, the European Union and its member countries consider it necessary to create a coordinated, efficient and effective response to these threats. Indeed, hybrid threats are mainly directed against democratic societies, often targeting democratic processes and institutions, which can undermine public trust in democratic systems. The fight against hybrid threats is therefore crucial for maintaining the stability and integrity of democratic societies within the European Union.

KEYWORDS: European Union, hybrid threats, democratic society, processes.

INTRODUCTION

In the era of continuous deterioration of the global and regional security environment, deterioration of the security situation in the immediate and distant neighborhood of the European Union (hereinafter referred to as "EU" or "Union"), deterioration of relations between states, especially between powers due to deepening geopolitical and geostrategic competition, as also the growth of complex asymmetric security threats, including the return of high-intensity conflict to the European continent, associated with unjustified and unprovoked military by Russia's aggression against Ukraine, a whole series of challenges arise for the EU (and implicitly its member states) regarding the ability to protect its interests and ensure its internal and external security. Especially if these challenges are connected with hybrid activities based on the power ambitions of some states and their efforts to exert economic, energy or other pressure on the Union, with interstate and national civil conflicts on the borders of the EU and beyond, and sources of tension and instability that lead to political, religious or ethnic oppression, humanitarian suffering and forced displacement of millions of people. In addition, the negative consequences of activities, conflicts and instability have been deepened in recent years by the multiplier effect resulting from ongoing climate changes.

All the above-mentioned aspects, but especially the hybrid activities conducted in the so-called gray zones [2]- implemented by state and non-state actors - lead to the fact that the

[2]The gray zone is a space in which a political and informational war is conducted, using the ambiguity of national and international law, and the activities of a state that harm another state are carried out, while from the legal point of view these are not acts of war, but acts below the threshold of armed conflict (NBU, 2024). The gray zone is the space between peace and war in which state and non-state actors compete with each other, or describes a situation where it is not clear whether something is legal or illegal, acceptable or unacceptable, etc. (Cambridge Dictionary , (2024).

current security environment has become much more complex, volatile and fragmented than ever before. Local and regional instability, fueled by dysfunctional governance and the questioning of democratic values, growing inequalities and political, religious and ethnic tensions, together with geopolitical and geostrategic rivalries, are increasingly affecting the effects of unconventional and transnational threats, ultimately undermining the ability of the EU multilateral system to prevent crises and mitigate them (Bradford, 2023).

This is also why the EU began to mobilize resources much more intensively in 2016 to ensure a higher level of its security (Felcan, 2019; Murdza, 2019) and began to create new tools to combat hybrid threats. These actions are the Union's response to the destabilizing activities of Russia and China, as well as smaller states such as Belarus, Iran and North Korea, but also to the activities of non-state entities such as terrorist organizations and extremist groups. So far, the EU's efforts have mainly focused on combating disinformation and propaganda and on strengthening the protection of critical infrastructure against cyber attacks. In *the Strategic Compass*, adopted by the EU Council on 21 March 2022, less than a month after the Russian invasion of Ukraine, the focus is much more on increasing the resistance of states and societies to manipulation of information and interference in political processes, as well as on expanding the EU's ability support Member States in responding to crises caused by hybrid methods, techniques and tactics (EU, 2022).

A EUROPEAN APPROACH TO COMBATING HYBRID THREATS

In 2016, the EU, in a document entitled *Common framework for combating hybrid threats,* defined hybrid threats as *"a mixture of coercive and subversive activities, conventional and unconventional methods (diplomatic, military, economic, technological) that can be used in a coordinated manner by state or non-state actors to achieve specific objectives, while these activities are below the threshold of officially declared war"* (EU, 2016). These types of activities can be used to pursue various strategic, operational and tactical goals with the aim of destabilizing states and interfering in their political, economic and social processes that affect the Union as a whole and individual member states. The EU's broad approach to this issue is based on the specifics of this phenomenon, especially the complexity of hybrid activities, their complexity and ambiguity. At the same time, the EU's response reflects the different security perspectives and priorities of the foreign and security policy of its member states. This flexible approach makes it possible to take into account threats from the east (Russia, Belarus) from the south (Iran, terrorist organizations, mass illegal migration) and threats with global reach (China).

The catalog of hybrid methods and tactics includes disinformation and propaganda activities, cyber attacks, interference in political processes (for example, elections, referenda, etc.), economic pressure, instrumentalization of irregular migration, state support of armed groups and employment of mercenaries, subversive information operations, terrorist activities or use of chemical, biological, radiological and nuclear substances. Hybrid methods can be used to varying extents and intensities and can be freely combined by state or non-state actors whose modus operandi are not the same. In addition, the catalog of hybrid warfare tools is "open" to any actions that may have disruptive effects on a societal level. The growing political rivalry with Russia (especially after the invasion of Ukraine) and China, the unstable situation in the EU's immediate and distant neighborhood, the militarization of vital sectors and environmental problems together with limited access to resources represent high risk factors for the security of the European area (EU, 2022).

Similarly, environmental protection issues can be used to create polarization and divisions within the EU. Climate change may in turn contribute to the destabilization of the Union's southern neighborhood, migration crises and the emergence of terrorist organizations. The instrumentalization of these phenomena by external actors (for example, the creation of

routes for the illegal introduction of migrants or the support of radical formations or groups to commit terrorist attacks) represents a direct threat to EU states. The catalog of hybrid threats is also expanded by emerging and disruptive technologies, including the development of artificial intelligence, providing advanced technical capabilities for disinformation and propaganda campaigns, as well as intelligence gathering and subversion activities. These considerations greatly complicate the development of response procedures to various hybrid attack scenarios, which, due to the cross-border and networked nature of hybrid threats, require a comprehensive and multidimensional approach to detection, early warning, countermeasures and emergency response (EC, 2022).

Since 2016, the EU has set itself the goal of developing capabilities to combat hybrid threats in four core areas, which are: (1) situational awareness; (2) building and implementing resilience policies; (3) facing and responding to crises (including overcoming their effects); and (4) cooperation and coordination with partners and international organizations (especially NATO). In this context, *the Strategic Compass* calls for strengthening these areas by creating new mechanisms and improving their use as part of the Union's coordinated response to hybrid crises (EU, 2022). In reality, the burden of responsibility for combating hybrid threats lies mainly with national security institutions (intelligence, security services, police and military), which have the legal and executive powers to do so (according to Article 4(2) of the EU Treaty). *The Strategic Compass* does not make any changes in this area, instead the tools developed under the EU's hybrid toolbox are intended to provide greater support to national efforts to combat hybrid threats and to coordinate Member States' joint actions to achieve synergies and more effective responses.

THE IMPORTANCE OF JOINT ACTIONS

In *the Strategic Compass*, the EU emphasizes the importance of continuing to strengthen the EU's intelligence capabilities to provide situational awareness and predict threats. The creation of hybrid mechanisms for sharing intelligence information about threats is of particular importance for determining the modus operandi of foreign intelligence services that are helpful in such actions. Improving the awareness of EU institutions and Member States in this area will increase the EU's ability to rapidly and adaptively detect and respond to crises caused by hybrid methods of hostile actors. Coordination of activities carried out by individual member states will also be improved. Activities in this area began in 2016 with the creation of the Hybrid Fusion Cell (HFC - Hybrid Fusion Cell) within the EU Intelligence and Situation Center (EU INTCENT – European Union Intelligence and Situation Centre). The cell consists of civilian and military analysts who are responsible for creating reports, briefings and analyzes within the framework of the Single Intelligence and Analysis Capacity (SIAC - Single Intelligence and Analysis Capacity) about hybrid threats that are identified at the level of the EU, member countries and its neighborhood (Bryjka, 2022). The studies are carried out on the basis of information from open and classified sources provided by the intelligence and security services of the Member States, EU agencies (such as the European Cybercrime Center, the European Counter-Terrorism Center or Frontex) and partner countries (such as Canada, Norway, etc.) With regard to cyber threat intelligence, the work of the cell is supported by representatives of the EU Cyber Emergency Response Team (CERT-EU – EU Computer Emergency Response Team). The exchange of sensitive information regarding, for example, the technical details of accounts, administrators, software or infrastructure used to carry out a disinformation operation is crucial in order to be able to attribute responsibility for these actions to a specific entity and impose sanctions on it (Polyakova, Fried, 2020).

The Hybrid Fusion Cell is the main component responsible for providing situational awareness to EU institutions and Member States. Its creation helped to increase the EU's ability to detect crises caused by hybrid threats in time, as well as to speed up and coordinate the joint

response of member states. An example in this regard is the EU's response (also in the form of effective strategic communication) to the migration crisis supported by Belarus in mid-2021 (with the support of the Russian Federation), which lasted for several months on the borders with Poland, Lithuania and Latvia. Despite Belarusian-Russian disinformation activities aimed at disrupting the interpretation and understanding of the border situation, the EU remained consistent and considered it a hybrid attack (Dyner, 2022).

In order to increase situational awareness of hostile information manipulation, the EU established a disinformation early warning system in March 2019. The exchange of information within this system takes place through contact points established in each country of the Union. The system was used in 2020 during the COVID-19 pandemic, when a wave of Russian and Chinese disinformation flooded the information space, undermining confidence in Western vaccines, EU institutions and vaccination strategies and fueling anti-vaccination movements and protests (Emmott, 2021). The main target of media attacks at that time was the European Medicines Agency. The system was used to exchange information between EU institutions and member states, representatives of the private sector and members of the G7 and NATO. Despite all the mechanisms and coordinated steps to fight disinformation, the wave of conspiracy theories spread by pro-Russian and pro-Chinese news channels (including " troll farms") caused a distortion of the perception of the current situation and distrust of the population towards vaccination (Colomina, 2021).

BUILDING POLICIES AND MECHANISMS TO RESIST HYBRID THREATS

The aim of strengthening the resilience of EU states and companies is to reduce their vulnerability to disinformation and propaganda by hostile entities and to develop the protection of critical infrastructure against cyber attacks, terrorism, subversion and sabotage. *The Strategic Compass* pays special attention to strengthening the EU's resistance to information manipulation and interference in political processes. The EU's approach to combating information manipulation consists of four elements adopted by the European Council in December 2018 in *the Action Plan on Disinformation*. It aims to: (a) increase the capacity of EU institutions to detect, analyze and debunk disinformation, (b) strengthen coordinated and collective responses to disinformation, (c) mobilize the private sector to combat disinformation, and (d) raise awareness and improve public resilience by supporting independent journalism, fact-checking initiatives and media education support (EC, 2018).

In 2015, in response to information and psychological operations by Russia with the aim of masking the actions carried out in Ukraine and in other areas of strategic interest, she was at the EU level within the framework of the European External Action Service (EEAS - European External Action Service) East StratCom task force created to monitor, analyze and respond to Russian propaganda and disinformation campaigns across a wide range of hybrid threats. East StratCom currently monitors intelligence reports published in more than 20 languages. By mid-May of this year, the team had identified almost 14,000 cases of Russian disinformation and cataloged them in the EUvsDisinfo database. In addition, the team organizes training for staff from partner countries, as well as activities to strengthen independent journalism and promote awareness of the EU and its policies in the Eastern Partnership countries (EEAS, 2021).

Similar tasks are carried out by the teams established in 2017, responsible for the Western Balkans region (Western Balkans Task Force) and the Middle East and North Africa region (Stratcom South Task Force), which focus on countering radicalization and propaganda and disinformation from Russia. China, Iran or Turkey. All three teams are part of the EEAS Division for Strategic Communication, which supports the EU institutions in planning strategic communication policies, strategies and tools. It also provides support (for example in the form of analysis and guidance on how to counter disinformation) to EU missions, operations and diplomatic missions under the EU's Common Security and Defense Policy, as well as

developing cooperation with partner countries, the G7, NGOs, civil society and by the private sector (for example, in the form of data acquisition using modern software and technologies). The aim of these activities is to raise public awareness and strengthen the resistance of countries neighboring the EU to disinformation (EEAS, 2022).

According to the EEAS, Russian disinformation represents the biggest threat to EU states due to its systemic nature. Russia has the resources to conduct disinformation campaigns as part of a long-term strategy to destabilize and disintegrate the Euro-Atlantic area. One of the most sensitive and vulnerable areas of misinformation in the functioning of EU states concerns democratic political processes, such as elections and referenda (Hajdúková – Šišulák; 2022; Hajdúková, 2023; Dušek, Kavan, 2024). To protect voters of EU member states from disinformation and cyber interference, CERT-EU created a specialized service Social Media Assurance Service to detect and remove accounts impersonating a real user.

The Union also adopted a "Code of Practice" that regulates EU countries' cooperation with the private sector regarding obligations for online platforms and the advertising industry to improve the transparency of political advertising, eliminate fake accounts and reduce incentives to spread misinformation. The Code has been adopted by major online service platforms such as Facebook, Google, Twitter and Microsoft, among others. They pledged to increase the transparency of political advertising and its financing and to block persons responsible for disinformation (EC, 2023).

The Strategic Compass announced the creation of a new mechanism to increase the situational awareness and resistance of the EU, its member states and their companies to manipulation of information and interference in political processes (FIMI - Foreign Information Manipulation and Interference Toolbox). The aim of the new cooperation platform is to standardize methods of data collection, analysis and exchange between member state governments, the private sector and civil society and international organizations on the tactics, techniques and procedures used by actors implementing hybrid threats. This approach will increase the EU's ability to identify and analyze disinformation campaigns in a timely manner, facilitate the collection of evidence of external interference in democratic political processes and standardize the methods of reporting such incidents (FIMI, 2023).

Strengthening the resilience of EU countries also covers key sectors such as cyber security, critical infrastructure, energy, transport, defence, the financial system, maritime security and space. This effort is primarily aimed at building the legal tools and capabilities needed to respond to incidents and crises caused by hybrid threats (especially in cyberspace) (Šišulák – Cíchová, 2019; Kozioł, 2022; Dušek, Kavan, 2023). A breakthrough in the EU's approach to cyber security was the adoption *of the Directive on the Security of Networks and Information Systems* in 2016. It obliges member states to guarantee common minimum standards for cyber security, including by adopting national rules, a cyber security strategy or creating computer incident response teams in within the European CERT network (EU, 2016).

The EU has also introduced mandatory reporting of cyber incidents for key service providers in the energy, transport, healthcare, banking and finance, water supply and digital infrastructure sectors. In addition to EU regulatory activities through the European Network and Information Security Agency (ENISA – European Union Agency for Cybersecurity) and the European Organization for Cyber Security (ECSO - European Cyber Security Organization) also supports research activities and cooperation between the public and private sectors. The common cyber defense capabilities of the member states are in turn being developed through four projects of the Permanent Structured Cooperation (PESCO - Permanent Structured Cooperation) on the exchange of information on cyber incidents, coordination of activities, joint support and response, as well as research and training (EU, 2019).

In December 2020, the Union adopted a new cyber security strategy, which aims to increase the resistance of member states to cyber attacks and better protect their critical

infrastructure (EC, 2020). An example of sectoral measures in this area is the EU cyber diplomacy toolkit, which contains measures that act as a deterrent to potential cyber attackers. Blacklisted entities – responsible for cyber-attacks or supporting cyber-attacks against EU states – will be sanctioned by banning entry into the EU and/or freezing their assets (Sadoian, 2024).

CRISIS PREVENTION AND RESPONSE

In accordance with *the Strategic Compass, the EU* emphasizes the importance of strengthening the Union's capabilities to respond to crises caused by an attack of a hybrid nature. That is also why it announced the creation of hybrid rapid response teams (EU Hybrid Rapid Response Teams) to support member states in hybrid attack situations. These teams represent one of the key tools to support EU Member States and partner countries in the fight against hybrid threats as part of the EU's hybrid toolkit. They should provide tailored and targeted short-term assistance to Member States, Common Security and Defense Policy operations and partner countries in the fight against hybrid threats and campaigns. In a deteriorating security environment with an increasing number of disinformation, cyber-attacks, attacks on critical infrastructure, instrumentalized illegal migration and interference in elections by state and non-state actors, hybrid rapid response teams should be an important new EU capability to face new and emerging threats (EU, 2024).

THE IMPORTANCE OF COOPERATION WITH NATO

The EU recognizes the importance of cooperation in the fight against hybrid threats with partners such as the United Nations ("UN") and the North Atlantic Treaty Organization ("NATO" or "Alliance"). In this regard, the Union attributes a key role especially to its relationship with NATO. It adopted *a Hybrid Threat Strategy* in 2015, which has three components: (a) preparing for hybrid attacks by improving reconnaissance and early warning capabilities, (b) strengthening critical infrastructure protection and testing decision-making processes within the Alliance, and (c) deterring a potential aggressor by imposing sanctions and maintaining uncertainty about the nature of the response and defending allies in the event of hybrid aggression (NATO, 2024).

In joint declarations from 2016 and 2018, the Union and the Alliance have drawn up a list of 74 joint actions in the security dimension, of which more than 20 are related to the fight against hybrid threats. The emphasis is mainly on recognizing this phenomenon, increasing situational awareness, building the resilience of society, protecting critical infrastructure and responding to emergency situations caused by hybrid threats (NATO, 2016 and 2018). Both organizations are also working on the implementation of joint initiatives based on systemic mechanisms of cooperation between their own employees at three interdependent levels: expert, intermediate (within the EU-NATO core group) and strategic (within the EU-NATO steering group). Through informal collaboration, the organizations have developed a common operational protocol to share knowledge about hybrid operations and coordinate the responses of both institutions.

The first joint initiative of the EU and NATO in the field of combating hybrid threats was the establishment of the European Center of Excellence for Countering Hybrid Threats in Helsinki in 2016, which provides expert and advisory support as well as a platform for sharing experience and information on hybrid threats. (Hybrid CoE, 2024). The Helsinki Center of Excellence contributes to current situation awareness for both organizations, as does the EU Hybrid Fusion Cell or its counterpart the Alliance Hybrid Analysis Department (NATO Hybrid Analysis Branch) operating within the Joint Intelligence and Security Division (JISD - Joint Intelligence and Security Division). Both structures have well-established working relationships through monthly staff exchanges. Both departments also prepare joint threat assessments (parallel and coordinated assessments) for the analysis of hybrid threats. Similar

cooperation is also developing between the East StratCom working group and the NATO Center of Excellence for Strategic Communication (StratComCoE - NATO Center of Excellence for Strategic Communication) in Riga, developing joint training materials, disinformation response courses and other tools for both EU and NATO personnel.

On a practical level, the EU Hybrid CoE in Helsinki is responsible for organizing workshops, seminars and exercises, which include simulations of the meetings of the North Atlantic Council (NAC) and the Political and Security Committee (PSC). Committee during hybrid attacks. Since 2017, the Union and the Alliance have been conducting NATO's Integrated Crisis Management Exercise (CMX) in the format of parallel and coordinated exercises to test the ability to respond to crises (including hybrid events) through a common operational protocol. Organizations are also looking for opportunities for joint (complementary) responses to threats in cyberspace, facilitated by joint training and exercises (e.g. Cyber Phalanx, Locked Shields or NATO Cyber Coalition), exchange of information and doctrinal documents, education, etc. The aforementioned cooperation takes place, among other things, through the European Defense Agency (EDA) and the NATO Cooperative Cyber Defense Center of Excellence in Tallinn. One of its important elements is cooperation in the technological field, including the exchange of experience and practices between CERT-EU and the NATO Computer Incident Response Capability (NCIRC) at the Supreme Headquarters Allied Powers Europe (SHAPE).

CONCLUSION

Creating a set of tools through which the EU is able to respond to hybrid threats strengthens the Union's ability to face these types of threats and respond promptly to them. The comprehensive set of measures to combat hybrid threats – developed since 2016 – is characterized by both flexibility of response and openness to identifying new methods and hybrid tactics used by both state and non-state actors. The obligation to respond to hostile hybrid actions rests with the member states in accordance with Article 4 par. 2 of the EU Treaty, while the role of the Union is to support them and coordinate common responses to crises. The implementation of new tools and modus operandi will, among other things, increase the situational awareness and resistance of EU institutions, member states and their companies to the manipulation of information and foreign interference in democratic processes.

Thanks to multilateral intelligence cooperation, the establishment of the Hybrid Fusion Cell and the early warning system against disinformation, the Union has significantly improved its situational awareness. The complexity of hybrid threats and the expected expansion of sectors of strategic interest (including health security, climate change, environmental protection or new technologies) call for the need to strengthen the analytical capabilities of these structures by increasing the number of employees and financial resources. It is in the interests of Slovakia and the Czech Republic – as EU and NATO member states – to actively participate in the activities of these institutions and to have their representatives in their structures (in executive and management positions) in the form of diplomats, military and civilian specialists and experts in the field).

Participation in the activities of EU and NATO institutions aimed at combating hybrid threats is important for Slovakia, the Czech Republic, and other member states for several reasons. Allows:

- Ensuring a higher level of security: Hybrid threats, which include cyber attacks, disinformation, economic pressures and other non-conventional forms of threat, pose a significant risk to national security. Cooperation within the EU and NATO enables member states to better face these threats and protect their population and infrastructure.

- Sharing of information and resources: Membership in the EU and NATO provides access to extensive sources of information and intelligence. Cooperation with these organizations enables more effective monitoring and prevention of hybrid attacks.

- Common defense and solidarity: EU and NATO member states can count on the support of other member states in the event of a hybrid attack. Solidarity and common defense are the basic principles of these organizations, which increases their security and defense.

- Strengthening cyber security: Cyber attacks are among the most significant forms of hybrid threats. The EU and NATO invest significantly in cyber defense and security. Participation in these initiatives and projects allows Member States to gain access to the latest technologies and expertise in cyber security.

- Increasing societal resilience: Hybrid threats are often aimed at destabilizing society through disinformation and propaganda. Cooperation within the EU and NATO helps member states build the resilience of their own society and population against these attacks, for example through educational programs and support for independent media.

- Protection of economic interests: Hybrid threats can also have serious economic consequences, for example through attacks on critical infrastructure or market manipulation. Membership in the EU and NATO enables member states to protect their economic interests and ensure economic stability.

- Increasing political stability: The stability of the political system is crucial for the functioning of the state. Hybrid threats such as cyber-attacks, the spread of disinformation and the manipulation of electoral processes can threaten democratic institutions. Cooperation within the EU and NATO strengthens the ability to protect democracy and political stability.

- Exchange of experience and best practices: Cooperation with other EU and NATO member states enables the exchange of experience and best practices in the fight against hybrid threats. Member States can thus gain valuable knowledge and experience and adapt it to their specific situation.

- Access to financial and technical resources: Participation in EU and NATO initiatives can provide member states with access to greater financial and technical resources needed to strengthen their security, which may include investment in infrastructure, training, development of new technologies, etc.

In general, it can be concluded that cooperation within the EU and NATO in the fight against hybrid threats is strategically beneficial for all member states, because it strengthens their capabilities and capacities to face not only current threats, but also future challenges related to the hybrid activities of hostile state and non-state actors.

REFERENCES AND SOURCES USED:

1. BRADFORD, A. (2023): The European Union in a globalised world: the " Brussels effect ". In *Le Groupe d'études geopolitiques*, 2023. [online]. [cit. 2024-07-4]. Available from: <https://geopolitic.eu/en/articles/the-european-union-in-a-globalised-world-the-brussels-effect/>.

2. BRYJKA, F. (2022): Tracing the Development of EU Capabilities to Counter Hybrid Threats. In *The Polish Institute of International Affairs*, 2022. [online]. [cit. 2024-07-06]. Available from: <https://pism.pl/publications/tracing-the-development-of-eu-capabilities-to-counter-hybrid-threats>.
3. Cambridge Dictionary. (2024): Grey zone. In *Cambridge Dictionary*, 2024. [online]. [cit. 2024-07-04]. Available from: <https://dictionary.cambridge.org/dictionary/english/grey-zone>.
4. COLOMINA, C. (2021): The impact of disinformation on democracy processes and human rights in the world. In *Policy Department for External Relations*, 2021. [online]. [cit. 2024-07-06]. Available from: <https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf>.
5. DUŠEK, J. – KAVAN, Š. (2023). Disinformation like component hybrid threats look students of VŠERS. In *Interpolis*, 2023, p. 7-25. Banská Bystrica: Belianum – Matej Bel University Publishing House, 2023. ISBN 978-80-557-2098-2.
6. DUŠEK, J. – KAVAN, Š. (2024). Disinformation like component hybrid threats - a Czech-Slovak perspective. In *Auspicia*, 2024, vol. 21, no. 1, p. 7-25. ISSN 2464-7217. DOI: 10.36682/a_2024_1_1
7. DYNER, AM (2022): he Border Crisis as an Example of Hybrid Warfare. In *The Polish Institute of International Affairs*, 2022. [online]. [cit. 2024-07-06]. Available from: <https://www.pism.pl/publications/the-border-crisis-as-an-example-of-hybrid-warfare>.
8. EEAS. (2021): Questions and Answers about the East StratCom Task Force. In *Europe External Action Service*, 2021. [online]. [cit. 2024-07-06]. Available from: <https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en>.
9. EEAS. (2022): Tackling disinformation: Information on the work of the EEAS Strategic Communication division and its task forces (SG.STRAT.2). In *Europe External Action Service* , 2022. [online]. [cit. 2024-07-06]. Available from: <https://www.eeas.europa.eu/countering-disinformation/tackling-disinformation-information-work-eeas-strategic-communication-division-and-its-task-forces_und_en?s=2803>.
10. EK. (2018): Action Plan on disinformation: Commission contribution to the European Council. In *Europe Commission*, 2012. [online]. [cit. 2024-07-05]. Available from: <https://commission.europa.eu/publications/action-plan-disinformation-commission-contribution-european-council-13-14-december-2018_en>.
11. EK. (2020): New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. In *Europe Commission*, 2020. [online]. [cit. 2024-07-07]. Available from: <https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391>.
12. EK. (2023): Code of Practice on Disinformation: New Transparency Center provides insights and data on online disinformation for the first this time. In *European Commission*, 2023. [online]. [cit. 2024-07-06]. Available from: <https://digital-strategy.ec.europa.eu/en/news/code-practice-disinformation-new-transparency-centre-provides-insights-and-data-online>.
13. EMMOTT, R. (2021): Russia, China sow disinformation to undermine trust in Western vaccines. In *Reuters*, 2021. [online]. [cit. 2024-07-06]. Available from: <https://www.reuters. com/world/china/russia-china-sow-disinformation-undermine-trust-western-vaccines-eu-report-says-2021-04-28/>.
14. EU. (2012): Treaty on European Union. In *Official Journal of the European Union*, 2012. [online]. [cit. 2024-07-05]. Available from: <https://eur-lex.europa.eu/resource.html?uri=cellar: 2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0011.02/DOC_1&format=PDF>.

15. EU. (2016): Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. In *Eur-Lex*, 2016. [online]. [cit. 2024-07-06]. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148>.
16. EU. (2016): Joint Framework on countering hybrid threats and European Union response. In *Eur-Lex*, 2016. [online]. [cit. 2024-07-05]. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018>.
17. EU. (2019): Complementary efforts to enhance resilience and counter hybrid threats – Council Conclusions (December 10, 2019). In *Council of the European Union*, 2019. [online]. [cit. 2024-07-07]. Available from: <https://data.consilium.europa.eu/doc/document/ ST-14972-2019-INIT/ en / pdf >.
18. EU. (2022): A Strategic Compass for Security and Defense - For a European Union that protect its citizens, values and interests and contributes to international peace and security . In *Council of the European Union*, 2022. [online]. [cit. 2024-07-05]. Available from: <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf>.
19. EU. (2024): Hybrid threats: Council paves the way for deploying Hybrid Rapid Response Teams. In *Council of the European Union*, 2024. [online]. [cit. 2024-07-07]. Available from: <https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/hybrid-threats-council-paves-the-way-for-deploying-hybrid-rapid- response-teams/>.
20. FELCAN, M. 2019. EU internal security and common security policy. In *Current problems resonating in Europe - a collection of contributions from an international scientific conference*. Bratislava: Police Academy, 2019. ISBN 978-80-8054-826-1.
21. FIMI. (2023): Foreign Information Manipulation and Interference. In *Disinformation.ch* 2023. [online]. [cit. 2024-07-06]. Available from: <https://www.disinformation.ch/ EU_Foreign_Information_Manipulation_and_Interference_(FIMI).html>.
22. HAJDUKOVÁ, T. (2023). Techniques for Manipulating Public Opinion in the Online Space During an Election Campaign as a Hybrid Threat. In *Academic Journal of Interdisciplinary Studies*, 2024, vol. 13, no. 1, pp. 14-23. ISSN 2281-4612. DOI: https://doi.org/10.36941/ajis-2024-0002
23. HAJDÚKOVÁ, T. - ŠIŠULÁK, S. (2022). Abuse of modern means of communication to manipulate public opinion. In: *INTED 2022: International Technology, Education and Development Conference - Conference Proceedings*. Barcelona: IATED, 2022, pp .1992-2000. ISBN 978-84-09-37758-9.
24. Hybrid CoE. (2024): What is Hybrid CoE? In *European Center of Excellence for Countering Hybrid Threats*, 2024. [online]. [cit. 2024-07-08]. Available from: <https://www.hybridcoe.fi/about-us/>.
25. KOZIOL, A. (2022): Strategic Compass: Towards EU Space Strategy for Security and Defense. In *Polish Institute of International Affairs*, 2022. [online]. [cit. 2024-07-06]. Available from: <https://pism.pl/publications/strategic-compass-towards-eu-space-strategy-for-security-and-defence>.
26. A short glossary of hybrid threats. (2024): The Gray Zone. In *National Security Office*, 2024. [online]. [cit. 2024-07-04]. Available from: <https://www.nbu.gov.sk/kratky-slovnik-hybridnych-hrozieb/>.
27. MURDZA, K. 2019. Defense awareness of the population as part of the EU security environment. In *Bezpečná společnost 2019 – proceedings from the international conference*. České Budějovice. college of European and regional studies, 2019, p. 35-43. ISBN ISBN 978-80-7556-056-8.
28. NATO. (2016): Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaties

Organization. In *the North Atlantic Treaties Organisation*, 2016. [online]. [cit. 2024-07-07]. Available from: <https://www.nato.int/cps/en/natohq/official_texts_133163.htm>.
29. NATO. (2018): NATO and EU leaders sign joint declaration. In *the North Atlantic Treaties Organisation*, 2018. [online]. [cit. 2024-07-07]. Available from: < https://www.nato.int/cps/en/natohq/official_texts_133163.htm > .
30. NATO. (2023): Joint Declaration on EU-NATO Cooperation. In *the North Atlantic Treaties Organisation*, 2023. [online]. [cit. 2024-07-07]. Available from : < https://www.nato.int/cps/en/natohq/official_texts_210549.htm > .
31. NATO. (2024): Countering hybrid threats. In *the North Atlantic Treaties Organisation*, 2024. [online]. [cit. 2024-07-07]. Available from: <https://www.nato.int/cps/en/natohq/topics_156338.htm>.
32. POLYAKOVA, A., FRIED, D. (2020): Democratic Offense Against Disinformation. In *Center for European Policies Analysis*, 2020. [online]. [cit. 2024-07-06]. Available from: <https://cepa.org/comprehensive-reports/democratic-offense-against-disinformation/>.
33. SADOIAN, L. (2024): The EU Cyber Diplomats Toolbox: Shaping Global Cybersecurity Standards. In *UpGuard*, 2024. [online]. [cit. 2024-07-07]. Available from: <https://www.upguard.com/blog/eu-cyber-diplomacy-toolbox>.
34. ŠIŠULÁK, S. – CICHOVÁ, M. 2019. Fake news and propaganda in cyberspace. 2019. In *Current challenges of cyber security in the conditions of security components: collection of contributions from a scientific conference with international participation*. Bratislava: Police Academy, 2019, p. 156-167. ISBN 978-80-8054-819-3.
35. ZAPLATYNSKYI, V. – URIADNIKOVA, I. 2019. Pyramid of Safety Realization of Needs. In *Bezpečná společnost 2019 – proceedings from the international conference*. České Budějovice. college of European and regional studies, 2019, p. 61-73. ISBN ISBN 978-80-7556-056-8.

CONTACT INFORMATION

colonel gst . with doc. Ing. Radoslav IVANČÍK, PhD. et PhD., MBA, MSc .
Police Academy in Bratislava
Sklabinská 1, 935 17 Bratislava
Slovak Republic
radoslav.ivancik@akademiapz.sk
ORCID ID – 0000-0003-2233-1014

WAR STATE AND STATE DEFENSE UNDER THE CONDITIONS OF THE CZECH REPUBLIC

Eva STÝBLOVÁ, Štěpán KAVAN

České Budějovice, Czech Republic

https://doi.org/10.36682/SSS_2024_4

ABSTRACT: The text deals with the issue of the state of war and state defense in the conditions of the Czech Republic, while examining the legal, organizational and crisis aspects of this area. In the introduction, the legal regulation of the state of war in the international and national context is analyzed, with an emphasis on international humanitarian law and its principles of ius ad bellum and ius in bello . The text also deals with the specifics of the defense mechanisms of the Czech Republic, including the government's organizational measures pursuant to Act no. 222/1999 Coll. on ensuring the defense of the state. Key attention is paid to the relationship between the state of war and crisis management, where the duties and roles of public administration bodies, including central crisis staffs, are emphasized. The analysis also includes an evaluation of the limits resulting from legal restrictions on human rights during the state of war, including measures related to freedom of movement and assembly. The text focuses on the importance of civil society in mitigating the effects of war, providing aid and post-war reconstruction. In conclusion, he emphasizes the importance of coordination and preparedness for war conflicts as key elements of the effective defense of the state.

KEY WORDS: State Defense, Martial Law, Czech Republic, Crisis Management, International Humanitarian Law

INTRODUCTION

War and armed conflicts represent serious phenomena of international law and politics. Although they are often seen as catastrophic events, there are precise legal terms that define them and theories that try to explain their nature and causes. In this text, we will focus on the legal aspects of war and armed conflicts, including their classification and regulation within international law, as well as on the basic theoretical approaches that attempt to explain them.

War as a concept has historically been vaguely defined, leading to many misinterpretations. However, after the adoption of the UN Charter in 1945, the rules governing the use of force became the main pillars of international law. The key principle is the prohibition of aggression, enshrined in Article 2 para. 4 of the UN Charter, which prohibits states from threatening or using force against the territorial integrity or political independence of another state (Schrijver, 2021).

According to the Geneva Conventions of 1949 and their Additional Protocols (1977), armed conflict is divided into international armed conflict (IAC) and non-international armed conflict (NOC). MOZ involves clashes between two or more states, while NOC refers to conflicts between a state and non-state armed groups or between these groups within a state's territory (ICRC, 2020).

Other legislation includes, for example, the Rome Statute of the International Criminal Court (1998), which defines war crimes and provides a legal framework for their prosecution. A key distinguishing feature of a war conflict is the intensity of the fighting and the organization

of the parties involved. For example, short-term riots or protests are not considered armed conflicts (Sassòli, 2019).

Legal regulation of war

The legal regulation of war is based on two main branches of international humanitarian law (IHL): ius ad bellum and ius in bello.

Ius ad bellum sets out the conditions under which war can be launched. The fundamental exceptions to the prohibition of the use of force under the UN Charter are the right to self-defense (Article 51) and collective security measures authorized by the UN Security Council (Gray, 2018). Ius in bello focuses on the rules of warfare and the protection of victims of conflict. The Geneva Conventions and other instruments of IHL regulate the conduct of parties to a conflict, including the prohibition of attacks on civilian populations, the use of prohibited weapons, and obligations to treat prisoners of war humanely (Henckaerts et al., 2005).

Despite these rules, many conflicts are marked by war crimes and other violations of IHL. An example can be the use of chemical weapons in the Syrian conflict, which was identified as a violation of the Chemical Weapons Convention of 1993 (UNSC, 2017).

Theoretical approaches to war

Various theories of international relations contribute to understanding the reasons why wars occur:

Realism: Realists see war as a natural consequence of the anarchic nature of the international system. According to this theory, states strive for power and security, which often puts them in conflict with other states (Mearsheimer, 2001).

Liberalism: Liberal theorists emphasize the importance of institutions, trade, and democracy in preventing conflict. For example, the democratic peace argument asserts that democratic states do not wage war among themselves, indicating the importance of the internal organization of states (Doyle, 1983).

Constructivism: This theory emphasizes the role of ideas, normative structures, and identity in international relations. According to constructivists, war is not inevitable, but is the result of specific social constructions (Wendt, 1999).

Marxist and Critical Theories: Marxist approaches see war as a consequence of economic inequality and capitalist expansion. Conflicts are seen here as a tool of imperialist control or competition for resources (Lenin, 1917).

Current challenges and legal dilemmas

Contemporary armed conflicts bring new challenges to international law and theory. The role of non-state actors such as terrorist organizations or private military companies is growing, complicating the application of traditional IHL rules. Another problem is the use of new technologies, such as autonomous weapons and cyber attacks, to which current legal norms often do not respond (Schmitt, 2013).

STATE DEFENSE UNDER THE CONDITIONS OF THE CZECH REPUBLIC

State defense is a set of measures to ensure sovereignty, territorial integrity, the principles of democracy and the rule of law, the protection of the lives of residents and their property from external attack. State defense includes the construction of an effective state defense system, the preparation and use of adequate forces and means, and participation in the collective defense system (Act 222/1999 Coll.).

The management and organization of the defense of the state includes the construction, preparation and management of the armed forces, the operational preparation of the state territory, the planning of the defense of the state and measures in the national economy and in

all areas of public life in order to ensure the defense of the state. The government is responsible for preparing and ensuring the defense of the state (Act 222/1999 Coll.).

Government to ensure the defense of the state in peace (Act 222/1999 Coll.):

- evaluates the risks of threats to the state that may be the cause of an armed conflict, and takes the necessary measures to reduce or eliminate these risks,
- evaluates the state's level of readiness to ensure its defense and, in connection with this, submits a report to the President of the Republic and the Chambers of Parliament on the facts found and proposed measures to strengthen the state's defense capability,
- approves the strategic concept of state defense,
- governs state defense planning, determines the content of individual state defense plans and the time stages for their processing,
- decides on the basic measures of preparing the state for defense and its organization,
- decides on the basic directions of the construction, preparation and use of the armed forces and on ensuring the defense of the state,
- approves the concept of mobilization of the armed forces,
- decides on the verification of measures for securing the defense of the state,
- approves the concept of preparing citizens for the defense of the state,
- sets tasks for ministers, heads of other administrative offices and territorial self-governing units in the exercise of their delegated powers to implement their decisions in ensuring the defense of the state,
- decides on other unpredictable tasks necessary to ensure the defense of the state.

Government to ensure the defense of the state in a state of threat to the state or in a state of war (Act 222/1999 Coll.):

- draws conclusions from the military- political assessment of international relations and decides on the implementation of the necessary measures to avert armed conflict and to increase readiness for the defense of the state,
- decides on measures for the effective functioning of the state defense system,
- decides on priorities for the fulfillment of tasks related to ensuring the defense of the state,
- decides on measures necessary for the conduct of war,
- it uses the Central Crisis Staff, established according to a special legal regulation, to fulfill its tasks in ensuring the defense of the state.

Relationship to crisis management

Central administrative offices, administrative offices and bodies of territorial self-governing units are obliged to cooperate with each other and to exchange information from the information systems they manage to the extent necessary when fulfilling the tasks of ensuring the defense of the state. When performing the tasks of ensuring the defense of the state, they use workplaces of crisis management, working and advisory bodies established according to special legal regulations, information systems of crisis management, operated according to a special legal regulation, and unified geographical data in accordance with a special legal regulation. Mutual cooperation and exchange of information is coordinated by the Ministry (Act 222/1999 Coll.).

In a state of threat to the state declared in connection with ensuring the defense of the Czech Republic against external attack and in a state of war, the crisis management authorities can also order measures according to a special legal regulation. Crisis plans drawn up according to a special legal regulation for a state of threat to the state declared in connection with ensuring the defense of the Czech Republic against external attack and during a state of war form a separate part of the state defense plan.

Limitation of basic human rights and freedoms

In order to ensure the defense of the state in a state of threat to the state or in a state of war, freedom of movement and residence and the right to peaceful assembly are restricted to the extent necessary. The restriction of freedom of movement and residence consists in the obligation to obey (Act 222/1999 Coll.):

- prohibition of entry into marked areas,
- an order to stay at the place of permanent residence or stay at the ordered place,
- prohibition of leaving buildings or structures designed to protect residents.

The restriction of the right to peaceful assembly consists in the obligation to obey the ban on convening assemblies in public spaces, including street parades and demonstrations. The provision does not apply to natural persons performing rescue work or ensuring the provision of assistance in the event of an immediate threat to health or life.

Local, personal and temporal scope and concrete determination of restrictions on human rights and fundamental freedoms are ordered by the government. The regulation is promulgated in the same way as a legal regulation and is published in the mass media and on the official boards of territorial self-governing units. Restrictions on human rights and fundamental freedoms take effect at the moment specified in the regulation.

THE RELATIONSHIP OF WAR AND CIVIL SOCIETY

War and civil society are phenomena that intertwine and influence each other. Civil society, understood as a set of organizations, associations and initiatives operating between the state and the individual, plays a key role in shaping responses to war conflicts, their impacts and solutions. This text focuses on three main areas: the impact of war on civil society, the role of civil society in war conflicts, and its role in post-war reconstruction.

The impact of war on civil society

Wars have a destructive impact on civil society because they destroy social structures, economies and trust between people. Armed conflicts often lead to the polarization and destabilization of society, with the erosion of basic civil institutions (Kaldor, 2003). For example, the civil war in Syria has caused widespread destruction of community organizations and led to the displacement of millions of residents, disrupting traditional forms of social cohesion (ICG, 2016).

However, some wars can also lead to the strengthening of certain forms of civic engagement. In crisis situations, people often come together in informal networks of solidarity to help each other. However, these forms of citizen initiative tend to be temporary and dependent on the intensity of the conflict and the availability of external support (Paffenholz, 2010).

The role of civil society in war conflicts

Civil society plays a key role in conflict prevention, mitigation and humanitarian assistance. Civil society organizations (CSOs) act as mediators between conflicting parties, often in the roles of informal negotiators or mediators of dialogue. An example is the organization Sant'Egidio, which played a significant role in the negotiation of the peace agreement in Mozambique in 1992 (Lederach, 1997).

During a conflict, ILOs can also be the main aid providers. Non-governmental organizations such as the International Committee of the Red Cross (ICRC) or Doctors Without Borders provide healthcare and protection to civilians in war-torn areas. These organizations often face challenges related to access to conflict-affected areas and the safety of their personnel (ICRC, 2020).

At the same time, civil society faces the dilemma of neutrality. Giving aid to one side can be seen as a political act, which can endanger the organizations themselves. For example, in conflicts like the one in Yemen, humanitarian organizations have been accused of supporting one of the parties, leading to restrictions on their activities (UNHCR, 2021).

Reconstruction of civil society after the war

Civil society has a key role in post-war reconstruction, particularly in promoting reconciliation, reconstruction and institution building. In post-conflict societies, civil society organizations are often involved in the reconstruction of infrastructure, assistance to victims and provision of basic services, which state institutions are often unable to provide (Paffenholz, 2010).

An important part of recovery is also the work of reconciliation between previously hostile groups. For example, in the Republic of South Africa, civil society organizations played a significant role in supporting the work of the Truth and Reconciliation Commission, which was instrumental in dealing with the legacy of apartheid (Tutu, 1999).

However, the recovery process can be complicated by lingering rivalries and mistrust. Experience from Bosnia and Herzegovina shows that if civil society is not sufficiently supported and coordinated with other actors, its influence can be limited and even deepen ethnic or political differences (Chandler, 2006).

Challenges and limitations

Despite its importance, civil society faces many challenges during and after wars. The main obstacles include:

- Lack of resources: Conflicts often disrupt funding and infrastructure, limiting the ability of IDPs to provide assistance (Kaldor, 2003).
- Political pressures: States and international organizations can instrumentalize civil society to achieve their own goals, reducing its independence (Chandler, 2006).
- Risks to actors: Activists and aid workers are often targeted during conflicts, limiting their ability to operate in the most affected areas (ICRC, 2020).

OPTIONS FOR PREPAREDNESS OF CIVIL SOCIETY FOR WAR

The preparedness of civil society for war includes the ability of organizations and communities to respond to conflicts, minimize their effects and provide basic functions even in crisis situations. This readiness becomes crucial in the context of the growing number of armed conflicts and their indirect consequences, such as migration crises or economic instability. This text analyzes three key areas of preparedness: conflict prevention, crisis management during conflict, and civil society engagement in post-conflict reconstruction.

Avoiding conflicts

One of the most effective forms of civil society preparedness is conflict prevention. Civil society can play a role in easing tensions and building trust between different groups through dialogue, education and promoting inclusive policies. Organizations like Search for Common For example, Ground focuses on facilitating dialogue between ethnic groups in areas with a high risk of conflict (Paffenholz, 2010).

Civil society can also contribute to conflict prevention by promoting transparency and accountability of governments. Anti-corruption initiatives such as Transparency International help to minimize systemic inequalities and the frustration of the population that often contributes to the outbreak of conflicts (TI, 2020). Education and awareness-raising about conflict-related risks is also a key aspect, helping communities to better understand their own vulnerabilities and options for prevention.

Crisis management during conflicts

During wartime conflicts, the preparedness of civil society is essential to ensure the basic needs of the population, the provision of humanitarian aid and the protection of the civilian population. One of the most important areas is the training and organization of communities for crisis scenarios, which includes, for example, evacuation plans, first aid and securing basic sources of food and water (ICRC, 2020).

Civil society organizations can also play a key role in providing information services. Access to verified information helps reduce chaos and the spread of misinformation that often complicates the situation in conflict areas. For example, during the war in Ukraine, civil society organizations created networks to disseminate accurate information about safe evacuation routes and provide humanitarian assistance (UNHCR, 2022).

Another important aspect is readiness for psychological support. Conflicts have a devastating impact on the mental health of the population, which is why it is important for civil society organizations to offer training to volunteers and professionals in crisis intervention (Wessells, 2009).

Post-war recovery

Civil society also plays an important role in post-war reconstruction, which includes rebuilding infrastructure, promoting reconciliation and rebuilding trust between communities. Previous experience shows that early involvement of civil society in recovery planning can prevent the deepening of social differences and tensions (Chandler, 2006).

One example of effective civil society involvement was post-war reconstruction in Rwanda following the 1994 genocide. Community organizations and local civil society initiatives played a key role in promoting reconciliation between survivors and perpetrators through traditional gacaca justice mechanisms and the promotion of collective economies (Clark, 2010).

Civil society can also contribute to the reconstruction of institutions and the provision of a legal framework that will prevent conflicts from re-emerging. In this context, it is essential to strengthen participatory decision-making so that all parts of society feel that their voice is heard and respected (Lederach, 1997).

Challenges in the preparation of civil society

Despite the importance of civil society preparedness, many organizations face a number of challenges. The main challenges include lack of funding and capacity, political obstacles and security risks. Wars often lead to the destabilization of state structures, which limits the ability of civil society to operate effectively. For example, in the conflict in Yemen, many humanitarian organizations have been targeted by attacks, severely limiting their ability to provide aid (UNHCR, 2021).

Another problem is insufficient coordination between individual actors. If the activities of civic organizations are not well synchronized, efforts may be duplicated or key areas that need assistance may be overlooked (Paffenholz, 2010).

CONCLUSION

War and armed conflict remain serious challenges for the international community. The legal framework provides the basis for their regulation, but its application is dependent on political will and the ability to ensure compliance. Theories of international relations offer different perspectives on the causes of conflicts and the possibilities of their resolution, but none of them provides a universal answer.

The relationship between war and civil society is complex and multifaceted. While wars often devastate civil society, they can also stimulate the emergence of new forms of solidarity and engagement. Civil society plays a key role in mitigating the impact of conflicts and promoting their resolution, as well as in restoring social order. However, for this role to be effective, greater support from the international community and stronger coordination between actors is needed.

Civil society preparedness for war is a crucial element in minimizing the damage caused by conflicts and promoting peace. The key to effective preparedness is the involvement of civil society in preventive measures, the development of crisis management and active participation in post-war reconstruction. Although they face a number of challenges, experiences from various conflicts show that civil society has the potential to significantly mitigate the negative effects of war on the population and contribute to long-term stability.

REFERENCES AND INFORMATION SOURCES

1. CLARK, P. (2010). The Gacaca Courts, Post- Genocide Justice and Reconciliation in Rwanda. Cambridge University Press.
2. DOYLE, MW (1983). Liberalism and World Politics. American Political Science Review.
3. GRAY, C. (2018). International Law and the Use of Force. Oxford University Press.
4. HENCKAERTS, J.-M., DOSWALD-BECK, L. (2005). Customary International Humanitarian Law. Cambridge University Press.
5. CHANDLER, D. (2006). Empire in Denial: The Politics of State-Building. Pluto Press.
6. CHANDLER, D. (2006). Empire in Denial: The Politics of State-Building. Pluto Press.
7. ICG (2016). Syria's Civil War: National and Regional Dimensions. International Crisis Group.
8. ICRC (2020). Commentary on the Geneva Conventions. International Committee of the Ed Cross.
9. ICRC (2020). International Humanitarian Law and the Challenges of Contemporary Armed Conflicts. International Committee of the Ed Cross.
10. ICRC (2020). International Humanitarian Law and the Challenges of Contemporary Armed Conflicts. International Committee of the Ed Cross.
11. KALDOR, M. (2003). New and Old Wars: Organized Violence in a Global Era. Polity Press.
12. LEDERACH, JP (1997). Building Peace: Sustainable Reconciliation in Divided Societies. United States Institute of Peace.
13. LEDERACH, JP (1997). Building Peace: Sustainable Reconciliation in Divided Societies. United States Institute of Peace.
14. MEARSHEIMER, JJ (2001). The Tragedies of Great Power Politics. W. W. Norton & Company.
15. PAFFENHOLZ, T. (2010). Civil Society and Peacebuilding: A Critical Assessment. Lynn Rienner Publishers.
16. PAFFENHOLZ, T. (2010). Civil Society and Peacebuilding: A Critical Assessment. Lynn Rienner Publishers.
17. SASSÒLI, M. (2019). International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare. Edward Elgar Publishing.
18. SCHMITT, MN (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press.

19. SCHRIJVER, N. (2021). The Use of Force under International Law. Cambridge University Press.
20. TI (2020). Corruption Perceptions Index. Transparency International.
21. TUTU, D. (1999). Well Future Without Forgiveness. Doubleday.
22. UNHCR (2021). Yemen Emergency. United Nations High Commissioner for Refugees.
23. UNHCR (2021). Yemen Emergency. United Nations High Commissioner for Refugees.
24. UNHCR (2022). Ukraine Situation Flash Update. United Nations High Commissioner for Refugees.
25. WENDT, A. (1999). Social Theory of International Politics. Cambridge University Press.
26. WESSELLS, M. (2009). Child Soldiers: From Violence to Protection. Harvard University Press.
27. Law no. 222/1999 Coll., on ensuring the defense of the Czech Republic. Collection of laws, amount 76/199 of 12/10/1999.

CONTACT INFORMATION

Mgr. Eva Stýblová
a) Faculty of Biomedical Engineering, CTU in Prague
Nám. Sítná 3105, 27201 Kladno, Czech Republic
b) Faculty of Health and Social Sciences, University of South Bohemia in České Budějovice
J. Boreckého 1167/27, 370 11 České Budějovice, Czech Republic
styblova.eva@gmail.com
ORCID iD – 0009-0001-7930-4044

PhDr. Štěpán Kavan, Ph.D.
Faculty of Health and Social Sciences
University of South Bohemia in České Budějovice
J. Boreckého 1167/27
370 11 České Budějovice; Czech Republic
stepan.kavan@email.cz
ORCID iD – 0000-0001-7997-8711

CONTRIBUTION OF THE EUROPEAN UNION CHIMERA PROJECT TO THE SECURITY OF THE CZECH REPUBLIC

Lubomír POLÍVKA

Prague, Czech Republic

https://doi.org/10.36682/SSS_2024_5

ABSTRACT: The aim of the article it's a present the content, significance and contribution of the CHIMERA project to the security of the Czech Republic. Following the current security situation in Europe, it was decided to tender the European Union project HORIZONT - CL3 – 2022 – DRS – 01-08 CHIMERA Comprehensive hazard identification and monitoring system for urban areas. This project is aimed at providing a breakthrough solution to be selected shortcomings and gaps in the CBRN security market. The main goal of the project is to develop a multi-platform CBRN command and control system for emergency services, dispatch centers and crisis management centers that will provide an overview of areas of interest, asset management and real-time data visualization. Ultimately, this will significantly increase the quality of the population's protection against the effects of CBRN substances, especially the protection of soft targets.
The Police Academy of the Czech Republic in Prague was invited to cooperate on this project.

KEYWORDS: Project, European Union, danger, urban areas, soft targets, emergency services, detection, command system, chemical weapons, biological weapons, radiological weapons.

INTRODUCTION

The current security situation in Europe and the world increases the risk of the possibility of using weapons of mass destruction in a terrorist or subversive manner. This situation was responded to in the European Union, among other things, by tendering the project HORIZONT -CL3-2022-DRS-01-08 CHIMERA - complex hazard identification system and monitoring system for urban areas. Work on the project is planned for the period from September 2023 to August 2026.

The CHIMERA project is focused on providing solutions to selected shortcomings and gaps in the CBRN security system. The project will develop a multi-platform CBRN command and control system for emergency services, dispatch centers and crisis management centers, which will provide an overview of areas of interest, asset management and real-time data visualization, as well as the development of a multi-purpose heterogeneous sensor node for CBRN detection, which will allow integration of commercially available detection devices. Furthermore, the project aims to implement real-time dispersion modeling software for chemical and radiological agents, which will provide dispersion models and source estimates with respect to urban environments, and integrate data algorithms combining data from different sensors from chemical, radiological or biological layers, in order to identify dangerous substances and reduce the number of false alarms. Ultimately, the CHIMERA project will create a database ready for commercial use combining the characteristics of substances C, B and RN. Thanks to these solutions, the results of the project will significantly strengthen both the operational capabilities of the first response and crisis management teams, as well as the safety of the on-site responders. All components developed within the project will function as separate units and as part of a whole combined system. In addition, the CHIMERA system will

have an open design, which will increase its interoperability and facilitate the integration of other existing systems. The project involves 11 researchers from EU countries (Germany, the Netherlands, Poland, Norway, the Czech Republic) and one from Japan.

On behalf of the Czech Republic, she was invited to cooperate on the project of the Police Academy of the Czech Republic in Prague. Within the Czech Republic, the General Directorate of the Fire and Rescue Service of the Czech Republic and other organizations dealing with this issue will be approached with the aim of informing about the project and involvement in possible professional consultations.

Overview of basic software products for modeling the spread of hazardous substances in open spaces and in urban areas.

Orientation overview of used systems and tools for modeling in the world.

Various programs and systems are being developed in the world, which have a very diverse and specific focus. Their outputs are usually displayed in text, but also in graphic form. Some are freely available and some are quite expensive.

Examples include:

- Aloha (US Environmental Protection agency)
- Dow index model for toxics
- Charm (Radian Corporation, USA)
- Degadis (US Coast Guard)
- Hegadas (SHELL)
- Denz / Crunch (SRD, UK)
- Haste (ERT, USA)
- Slab (Lawrence-Livermore National Laboratory, USA)
- Phast (Technica, UK)
- Trace (SAFER CORPORATION, USA)
- Drift (Germany, UK)
- Superatmos (AD Little).

Possible evaluation criteria and comparison of SW programs

As a rule, the following basic criteria are used:

- user friendliness,
- hardware support requirements,
- requirements for the user's knowledge and skills,
- the price of the SW tool and requirements for other subsequent expenses (updating data, installation, etc.),
- degree of practical use for users,
- range of required input data,
- the model's ability to calculate pollutant loss,
- the ability of the model to include in the calculations the relevant chemical processes taking place in the atmosphere,
- the ability of the model to calculate different durations of leaks,
- the size of the area for which the model can calculate pollutant concentrations,
- the ability of the model to include in the calculation the effect of the character of the surrounding terrain (i.e. buildings, forest, open landscape, etc.),
- format of output information, its comprehensibility and applicability for possible further use,

- model rating, experience with their use, etc. (e.g. references at the US EPA or in the works of recognized experts) [3].

Examples of programs used in the Czech Republic

In the Czech Republic, ALOHA is usually used with foreign programs. From the Czech programs, TerEx and ROZEX Alarm are usually used. TerEx is more widespread.

ALOHA[4]

ALOHA (Areal Locations of Dangerous Atmospheres) is a modeling program that estimates danger zones associated with the release of hazardous chemicals, including clouds of toxic gases, fires and explosions. A threat zone is an area where a hazard (such as toxicity) has exceeded a user-defined level of concern (LOC). ALOHA is part of the CAMEO software suite.

Key functions of the program

Generates a variety of scenario-specific outputs, including threat zones, threats at specific locations, and resource strength graphs. It calculates how quickly chemicals are escaping from tanks, ponds (on land and water) and gas pipelines and predicts how these release rates change over time.

It models release scenarios: clouds of toxic gases, BLEVE (explosiveness in vapors), jet aircraft fires, vapor cloud explosions, tank fires, etc. It evaluates different types of hazards (depending on the release scenario): toxicity, flammability, thermal radiation and overpressure.

It shows hazard zones on MARPLOT maps (and also on Esri 's ArcMap with the ALOHA ArcMap Import ToolExternal link and on Google Maps and Google Earth using the export as KML function). Works seamlessly with accompanying programs CAMEO Chemicals and MARPLOT; it can also be used as a standalone program.

ALOHA is one of the simple computer programs that can be used to calculate leaks of industrial chemicals and to model the spread of clouds of leaked substances into the environment. However, it is necessary to learn how to operate it.

TEREX – Terrorist Expert[5]

It evaluates the effects of the leakage of dangerous chemical and noxious substances or the occurrence of a booby-trapped explosive system. Database of dangerous substances, including characteristics, description, principles of first aid, method of decontamination, etc.

What it can do:

- Contains an extensive database of chemical substances.
- It models and simulates crisis situations.
- It enables quick decisions in the event of a crisis.
- It helps with planning, teaching and practice.

For whom it is intended:

- Enterprises
- Educational institution
- Self-government and state authorities
- IZS folders

[3]Regulators - Air. IOWA DNR. Iowa department of natural resources [online]. 2014 [cit. 2014-04-23]. Available from: http://www.iowadnr.gov/InsideDNR/RegulatoryAir/afo/files/section4

[4]https://www.epa.gov/cameo/aloha-software

[4] https://www.tsoft.cz/

The application can be further expanded with any amount and types of hazardous substances. Mathematical models can be adapted to a specific application in practice and chosen priorities.

Among the advantages of the TerEx program are its user-friendliness and intuitive control. Parameters can be selected directly from the offered options. A great advantage of this program is its functionality even with incomplete input.

ROZEX Alarm[6]

The ROZEX software contains a database of chemical substances (including integration with the MEDIS ALARM database of the company MEDISTYL, spol. s ro), the information range of the database of chemical substances is:

- Substance identification (name and synonyms, CAS, EC, EINECS, UN code identifiers),
- Classification of dangerous substances according to CLP, H-phrases, P-phrases,
- Physical-chemical properties,
- Instructions for intervention, extinguishing,
- First aid and medical treatment,
- Concentration limits of AEGL, ERPG, HAU and others.

The ROZEX software has computational functions for quantitative risk analysis:

- Source element models (one-time leakage, continuous leakage, hole leakage, puddle evaporation, instantaneous evaporation),
- PUFF / PLUME dispersion models,
- Fire models (pool fire, jet fire, BLEVE – fireball, flash fire)
- explosion models,
- Prediction of the range of emergency manifestations (toxic contamination, thermal radiation, flashfire range, overpressure wave),
- Modeling for toxicity reference values (AEGL, IDLH, HAU, IDLH), thermal radiation and overpressure.

The ROZEX software can be expanded with specific modules in the field of quantitative risk analysis and prevention of serious accidents:

- structured registration and passporting of operational areas, objects, equipment and technologies and dangerous chemical substances,
- identification and selection of risk sources according to Purple book / BEVI (Guidelines for Quantitative Risk Assessment, Purple book, CPR 18E, Committee for the Prevention of (Disasters)
- in the calculations of emergency planning and hazard zones using the method according to decree no. 226/2015 Coll.

The ROZEX software has user functions for printing and exporting calculations to the ESRI Shapefile format. The program has approximately 8,000 chemical substances in its database. The program has a total of nineteen types of emergency scenarios. The obtained outputs can then be exported to map documents.

Medis -Alarm [7]database of dangerous substances is one of the most widespread databases in the Czech Republic. It contains approximately 10,000 records of dangerous chemical substances and has been under construction since 1991. Initially, it was based on a list of approximately three thousand substances and dangerous goods according to the RID agreement,

[6]https://www.tlp-solutions.cz/produkty/software-rozex/

[7]Mika Otakar, Polívka Lubomír, Malinovský Karel. Matýz Tomáš. Important database of dangerous substances Medis-Alarm in the Czech Republic. Chemical Letters - volume 118. Prague 2024. ISSN 0009-2770.

which sets the conditions for transporting dangerous goods by rail, but over time other substances were added, which they figure in Czech and European legislation regulating the handling of dangerous substances and mixtures.

The database is intended mainly for IZS components and production companies, but also for distributors of chemical substances, state administration offices, students and others.

Medis -Alarm database has a multi -criteria search, currently around forty criteria, also part of this database are hygiene limits, recognized recommendations, symptoms and instructions for treatment plus links with Czech, Slovak and European legislation.

Examples of used programs in the EU and outside it

In the European Union, a number of tools are used to model the spread of dangerous substances and weapons of mass destruction (CBRN). Depending on the level of difficulty, they are available in price ranges from thousands to tens of thousands of Euros.

- ALOHA - Area Locations of Dangerous Atmosphere (USA)
- DEGADIS (USA) It is mostly used by the coast guard and in the gas industry.
- CHARM (USA) It is used for prognostic modeling of the consequences of chemical accidents. It requires trained specialized service. The program cooperates with the American crisis system EIS Infobook.[8]
- EFFECTS 4

It requires highly professional service. It evaluates exothermic and toxic manifestations of serious accidents without the possibility of graphically displaying the results on a map.

EOD Frontline / CBRNE Response[9]

It is an application for crisis management. It is primarily intended for events connected with pyrotechnic issues, but it can be used for chemical accidents. The EOD Frontline application uses three types of threat areas:

- Explosive zones for explosives.
- Areas threatened by chemical warfare agents (spread by weather effects).
- Areas threatened by industrial toxic materials (spread by weather effects).

The EOD Frontline application cooperates with NATO systems. It works with maps, can process messages, uses a communication module, etc. The program is suitable for communication within military and non-military crisis management.

Other programs:

- Phast (Great Britain),
- Sevex view (Belgium).
- Damage (Germany),
- Save (Germany).

Summary

From the above data, it follows that the use of software tools for quick forecasting and orientation in the seriousness of the incident and the direction and space of the spread of the dangerous substance is beneficial in the population warning system, the organization of the intervention of the components of the integrated rescue system (IZS) and the organization of the possible evacuation of people from the infected area.

[8]HRABĚ, Jan. Analysis of available SW for modeling the impacts of possible NL leaks into the atmosphere. Prague: T-Soft as 2006.

[9]EOD frontline. AURA, sro EOD Frontline: AURA [online]. 2014 [cit. 2014-04-23]. Available from: http://www.aura.cz/cz/eod-frontline.php

However, it is necessary to choose the relevant program according to the actual needs for which it will be used, taking into account other aspects of its use, such as the frequency of use, the ability of the operator to work with it, the possibility of using other related products, etc. In addition, in connection with the compatibility of the use of these tools across the EU, including communications with NATO in the case of CBRN use and military crisis situations, it appears appropriate to create a tool that could be used by all EU states. Experience with using existing programs can be used when creating this program. For a more accurate evaluation of the data, it would be necessary to include the possibility of calculating the spread of substances in residential areas, taking into account the characteristics of buildings, air turbulence in the streets, etc. From the point of view of its dissemination and use across all affected entities such as emergency services, crisis management authorities, industrial enterprises, etc. it would be most appropriate for it to be freely distributed according to the example of the ALOHA program.

The EU CHIMERA project is supposed to contribute to the overall improvement of this situation.

CHIMERA SYSTEM REQUIREMENTS

The user requirements were developed in accordance with the basic rules stated in the ISO IEC 29148:2018 standard together with intensive consultations with the members of the CHIMERA consortium responsible for the further design and development of the CHIMERA system. The defined functional requirements of the users further served as input for the gradual definition of key performance parameters for the CHIMERA system, which dealt with user requirements and performance goals for the EU-RION system. The prepared list of key performance parameters can be further expanded, verified and quantified through the cooperation of stakeholders/partners, both within the framework of the system design.

Starting the process is based on the following steps:

- analysis of the current state of modern CBRN systems;
- search for synergies between other CBRN projects,
- definition of operational context and inter-organizational integration;
- from seeking and verifying user requests;
- creation of relevant scenarios.

User requirements and features - general considerations

User requirements define the specific needs, expectations, preferences and limitations of the end users who work with the product. These requirements are a set of basic functions, properties and attributes that users expect from the system, viewed through the lens of the user environment. "User requirements" describe in detail what users require from the software.

Description of the system as such

The CHIMERA project will provide a breakthrough solution to selected shortcomings and gaps in the field of CBRN security. The aim of the project is to achieve this goal by developing a multi-platform command and control system for intervention components, operational centers and crisis management bodies, which provides:

- overview of areas of interest,
- overview of equipment,
- data visualization in real time,
- a multi-purpose heterogeneous sensor node for the detection of CBRNe agents enabling the integration of commercially available detection devices,
- software for modeling the spread of substances in real time and in 3D visualization using models and estimates of spread in the urban environment,

- implementation of data fusion algorithms combining data from different sensors from the chemical, radiological or biological layer enabling identification of agents and reduction of false alarms.

Ultimately, the CHIMERA project will create a database ready for commercial use, which will combine the properties of all substances. Thanks to these solutions, the results of the project will significantly improve both the operational skills of rescuers and teams for managing dangerous situations (emergency events, terrorist attacks, crisis situations), and the safety of personnel on site. All components developed in the project will be able to function as separate units and as part of the whole system. In addition, the CHIMERA system will have a user-friendly design that will increase its interoperability and facilitate the integration of other existing systems.

Visualization of data/information will be possible in real time (including threat maps, localization of sensors and their readings in real time).

The following main products will be developed:

Product 1: Heterogeneous sensor node (hardware and software):

A microcomputer device enabling the integration of multiple commercial CBRN sensors through dedicated adapters thanks to an open node interface. The node combines readings from connected sensors and runs data fusion algorithms (at the node level) to classify and identify CBRN hazards. The result is that a single node unit (with integrated sensors) is capable of intelligent sensing. The more units are integrated into the wireless network, the better coverage of the area of interest is ensured for the end user. The device will be powered by batteries.

Product 2: Adapters for detection devices (hardware and software):

The product is complementary to the sensor node. The adapter is designed for specific commercial sensors. Thanks to the design of the adapter, any commercial sensor can be integrated into the node. The purpose of the hardware adapter, which is connected to the communication interface of the given sensor, is to wirelessly transmit data from the sensors to the node, where the data is merged with the readings of other connected sensors and further processed. Dedicated adapters will be developed as part of the project.

Product 3: Device for detecting heterogeneous radiological danger (hardware):

The device contains a Geiger computer for calculating the dose rate and a spectrometer (eg cadmium and zinc telluride) for identifying nuclides. The combination of these two sensors is enclosed in one case. The Geiger computer enables a quick estimation of the dose rate even for unidentified nuclides. The purpose of the spectrometer as a complementary technology to the Geiger counter is to have more data to process to identify the radioactive nuclide. The detection device will also include a navigation module for accurate estimation of the current position. The device will be manual and will work on batteries.

Product 4: A program that calculates the dispersion of CBRN hazardous substances in the air based on source location, sensor node data and wind field data.

CONCLUSION

The aim of the previous chapters was to inform about existing systems and products for evaluating the spread and effects of dangerous substances, including CBRN. At the same time, to familiarize with the meaning and specific expected results and contribution of the CHIMERA project - Comprehensive hazard identification and monitoring system for urban areas. Its contribution is mainly technological improvement in the field of detection and evaluation of the spread of CBRN in accordance with European legislation, including the relevant EU directives, and the improvement of the ability of end users (i.e. rescuers, dispatchers and crisis management centers) using new detection, identification and monitoring products. Another added value of the system is the unification of the evaluation of the spread and effects of these

agents within the EU and thus a more unified, easier and more accurate transfer of information and mutual communication between individual states. If it were possible to ensure the free distribution of the main software products to the necessary users, then the level of protection of the population would also be increased with an emphasis on the area of warning and correctly chosen evacuation.

LITERATURE:

1. Mika Otakar, Polívka Lubomír, Malinovský Karel. Matyz Tomáš. An important database of dangerous substances Medis -Alarm in the Czech Republic. Chemical Letters - volume 118. Prague 2024. ISSN 0009-2770.
2. HRABĚ, Jan. Analysis of available SW for modeling the impacts of possible NL leaks into the atmosphere. Prague: T-Soft as 2006.
3. EOD frontline. AURA, sro EOD Frontline: AURA [online]. 2014 [cit. 2014-04-23]. Available from: http://www.aura.cz/cz/eod-frontline.php
4. Regulators - Air. IOWA DNR. Iowa department of natural resources [online]. 2014 [cit. 2014-04-23].
5. https://www.epa.gov/cameo/aloha-software
6. 4 https://www.tsoft.cz/
7. https://www.tlp-solutions.cz/produkty/software-rozex/

CONTACT INFORMATION

Ing. Lubomír POLÍVKA
Department of Crisis Management
Police Academy of the Czech Republic, Lhotecká 559/7, 143 01Prague 4
Polivka@polac.cz
ORCID – 0000-0001-8984-4565

LIFE IN KYIV DURING THE WAR

Vasyl ZAPLATYNSKYI, Inga URIADNIKOVA

Kyiv, Ukraine

https://doi.org/10.36682/SSS_2024_6

***ABSTRACT*:** The article provides a retrospective analysis of the events that took place in Kyiv during the full-scale war. A number of elements are described that are important during war. In particular, emphasis was placed on the evacuation of people from Kyiv and the return of people (re-emigration). A number of safety measures are shown. Functioning of educational, cultural, sports institutions. Operation of transport, including during the air alert period. Special attention is paid to the functioning of educational institutions, including preschool, secondary and higher institutions. The peculiarities of the operation of shops, pharmacies and other establishments are revealed. The article includes an analysis of life activities in conditions of insufficient supply of electricity. A comprehensive analysis of the events that took place in Kyiv makes it possible to assess the most important risks and draw conclusions about the main steps that must be taken during the war.

KEY WORDS: war, danger, Ukraine, Kyiv, population, war risks.

INTRODUCTION

The article presents materials that reflect a subjective, personal view of the events that took place and are taking place in Kyiv since the beginning of Russia's full-scale war against Ukraine. The text of the article does not claim to cover all aspects of life in Kyiv during the war, it is only a summary of what was available to the authors of the article. This is their vision, their understanding of the events that took place.

The relevance of the article is determined by the opportunity to assess the dangers and peculiarities of life during an emergency situation, which is war. The experience of Ukrainians and, in particular, the residents of Kyiv during the war is valuable not only for countries in which war may break out, but also for any country or area where this or that major emergency situation may arise.

All events in Kyiv can be divided into several stages: before the start of the war; the beginning of the war; the first month of the war; Kyiv and Ukraine during the war.

METHODOLOGY AND PURPOSE

The purpose of the article is to publish a study of life in Kyiv at various stages of a full-scale war. The task of the research is to show the risks of wartime, the actions of people that were carried out in order to prevent or eliminate war risks and their consequences. Among the methods used, observation, analysis of mass media messages and retrospective analysis were most used.

1. BEFORE THE START OF THE WAR

Probably the majority of Ukrainians did not believe in the beginning of full-scale Russian aggression against Ukraine until the last moment. However, there are no reliable statistical data on this issue. Of course, information about the possible beginning of the war circulated in certain areas, in particular, among the military and in the power structures and, of course, among

their acquaintances. Therefore, some people met the beginning of the war at workplaces in preparation for a military attack by Russia. But the absolute majority of the population of Ukraine did not expect large-scale military actions on the part of Russia. For the majority of the population, the announcement of the beginning of full-scale Russian aggression was a shock. Few people imagined that tanks would go to Ukraine and missile strikes would take place on military units and cities on the territory of Ukraine. Of course, hostilities have been taking place since 2014. At that time, Crimea was seized and fighting began in the Luhansk and Donetsk regions. But before the full-scale war, the intensity of hostilities in the east of Ukraine decreased significantly, and there was even a feeling that the war in the east of Ukraine might end in the near future. Of course, we all followed the actions of the presidents: President Poroshenko and his successor, President Zelensky, and the actions of politicians and diplomats. News has long become an important element of the life of the residents of Ukraine. The perception of the news and the perception of the situation before the war, which almost unambiguously pointed to the beginning of a large-scale war of Russia against Ukraine, was perceived differently by different strata, different age groups of the population of Ukraine and in different regions. It is worth recalling that the mentality of the older generation of Ukrainians was formed under the conditions of the Soviet Union, whose slogans, in particular, were brotherhood. Therefore, this category of the population was more skeptical about the start of a full-scale war between Russia and Ukraine. A significant number of immigrants from Russia in Luhansk and Donetsk regions, as well as in Crimea, contributed to the annexation of Crimea and the deployment of hostilities on the eastern borders of Ukraine. Analysts note that Ukraine had enough forces and means to counter the critical situation in the east of Ukraine in 2014, but due to a number of reasons, including the political and organizational nature of the situation, it was allowed to deteriorate. Many analysts note that the first armed demonstrations by Russian-backed separatists in the east of Ukraine could have been put down practically in the first month. However, time was lost.

A subjective assessment shows that Ukraine entered a full-scale war in 2022 much weaker than it was after the collapse of the Soviet Union. This situation was facilitated by the political decisions of the leadership, including the top and military leadership of Ukraine, and certain international influence. It should be recalled that after the collapse of the Soviet Union, Ukraine retained only 18% of the Black Sea Fleet, and 82% of the most combat-capable fleet remained in Russia. Ukraine renounced the status of a nuclear power and transferred its nuclear weapons to Russia in accordance with the Budapest Memorandum, which was signed on December 5, 1994 by Great Britain, the United States, Russia and Ukraine. This document should become a guarantee of the sovereignty and inviolability of Ukraine's borders and its integrity as a state. Questions still occasionally arise about whether Russia would have dared to annex Crimea, go to war in the east in 2014, and launch a full-scale attack in 2022 if Ukraine had remained a nuclear power. During the time of Ukraine's independence, armament issues were not dealt with sufficiently. There was a time when army property was widely sold off. Armaments, instead of being transferred to preservation, were destroyed. Warehouses with ammunition began to burn more often. In addition to the issue of armaments, it is necessary to take into account the fact that many Ukrainian soldiers were trained in Russia, and Russian soldiers were trained in Ukraine. Of course, under these conditions, it was quite easy for Russia to recruit supporters and conduct preparations for war.

As for the general economic situation in Ukraine, although it was not the best compared to advanced developed countries, it was not the worst either. In recent years, before a large-scale war, inflation almost stopped and the national currency, the hryvnia, became quite stable.

2. THE BEGINNING OF THE WAR

February 24, 2022 became a significant day for many people. Perhaps the Russians could have started the war a little earlier, but it was necessary to celebrate the "Day of the Defender of the Fatherland" - a holiday that has been preserved in Russia since the time of the Soviet Union.

Many Ukrainians received their first information through the mass media. Some woke up to rocket explosions. Someone outside the window saw tank columns moving from Russia to Ukraine. Someone was called by relatives or notified by neighbors. Shock and confusion were the first feelings for many. In addition, the question arose "how so, why?" to which there was no answer. Few people went to work in Kyiv. Many organizations and institutions urgently sent notices about the cancellation of the working day. However, there were organizations, including in the field of education, that demanded presence at workplaces. Thus, the residents of Kyiv were divided into two groups. The first part of the residents of Kyiv continued to work, and the other began to urgently evacuate to the west of Ukraine and abroad. It was possible to observe how at 7 o'clock in the morning (and maybe someone left even earlier) cars with people and things were already being loaded and going somewhere west. The transport arteries of the city were crowded. It is indicative that the journey from Kyiv to Lviv, which usually takes about 7-8 hours by car, increased even to several days during the evacuation. In a few days, hostilities broke out, including on parts of the Kyiv - Lviv - Chop and Kyiv - Warsaw roads. This situation made it difficult to leave Kyiv. Hiring a tow truck was very difficult and extremely expensive.

There were many people at the railway station. Of course, there were no more tickets in the western direction. The evacuation actually lasted quite a long time and had several waves. Even today, the evacuation continues from regions in which there is a high risk to life due to the increase in the intensity of shelling and the offensive of the Russian army. Today, there is also a hidden evacuation of young people abroad. Young people under the age of 18 go to study in vocational and technical and higher education institutions of Western countries, including Poland, Slovakia, the Czech Republic and other countries.

Of course, at first there was no organized infrastructure for receiving refugees, so those people who went first relied only on their own strength, the presence of acquaintances and relatives, etc. It should be noted that border crossing by men of draft age was still allowed in the first days of the war.

In the first days of the war, a significant part of the population remained in Kyiv. With the establishment of infrastructure for the reception of refugees in the western regions of Ukraine and abroad, it has become easier to evacuate. Ukrainian Railways has introduced a number of evacuation trains. Some of them brought people from the eastern regions, some went west from Kyiv to Ternopil, Lviv and other cities. It is worth noting that it was possible to go to the evacuation for free. Railway workers worked selflessly despite shelling and risks. Some of them died while performing their duties.

When asked about the number of people who remained in Kyiv at the peak of the evacuation (March 2022), we can frankly say that there are very few people left in Kyiv. The 16-story building, where the authors of the article lived, was practically empty. No more than 10% of residents remained in the building. Of course, the situation was different in other houses of Kyiv. However, there were not many people on the street either. The main reason for such a large evacuation from Kyiv was the hostilities that were taking place on the approaches to the capital. The line of military confrontation lay, practically, several kilometers from the capital. Russian troops were especially close in the north-western and eastern directions.

Media reports about a quick end to hostilities contributed to the temporary evacuation. People preferred to wait out the war in safe places. Information agencies and analysts of various kinds reported, at first, about two or three weeks of war, then a month, two months, and so on. This question worried and still worries all Ukrainians, that is why people listen to the predictions made today by politicians, analysts, journalists, and often astrologers and psychics.

Everyone had their own considerations regarding the choice between evacuation and continuing to live in Kyiv. Obviously, if the Ukrainians had not repelled the attacks of the Russians and they had not retreated from Kyiv, the flow of refugees from Kyiv would have been even greater.

People who remained in Kyiv on the first day of the war went to work or to shops. Many began to stock up on food. After all, the stories of grandparents who survived the Second World War were still very fresh. As people learned about the start of hostilities, queues in shops and supermarkets grew. Those people who came to supermarkets earlier had the opportunity to buy more goods, but already around 8 o'clock and at the beginning of 9 o'clock, the number of customers increased significantly and it was necessary to stand in a huge queue to get into the supermarket. They bought everything: matches, salt, sugar, bread, canned goods, products that can be stored for a long time, pasta, cereals, bottled water, hygiene products, including soap, detergents, toilet paper, napkins. Store shelves were quickly emptied. They bought everything that might be needed during the long absence of products and goods. It is worth noting that people were right because in the first two weeks the situation with the work of shops and supermarkets was very difficult. Many of them stopped working on the second day of the war. Some stores sold stocks of frozen products, in particular, frozen meat, frozen poultry and other products that were stored in large refrigerators in these stores. This was done in order to close the stores, because the prospect of further operation of the store or supermarket was very vague and many of them sold out and closed until a better time.

The shock of the first time affected the operation of all life support systems, but I must say that electricity, water, heating, television and radio functioned quite well.

3. LIFE IN THE FIRST WEEKS OF THE WAR

Russian aggression and the troops around Kyiv united Ukrainians in their desire to defend their country and Kyiv from invaders. Thousands of Kyivans came to military commissariats to sign up as volunteers for the army and territorial defense. There were a lot of people. Territorial defense units were quickly staffed. For those who came later, they wrote down their phone numbers and promised to contact them later. However, there was always work for those who wanted to help the country fight the enemy. People worked as volunteers. Sandbags were filled and placed on the streets. At enterprises, anti-tank barriers (hedgehogs) were welded. Almost all the streets of Kyiv were blocked by roadblocks, fortifications made of anti-tank hedgehogs and sandbags. It was very difficult to drive through the city, because there were only small roads that were controlled by the military and members of the territorial defense. People, whenever possible, helped the military. The number of volunteer organizations and their number has increased. Educational institutions often became centers for volunteers. Volunteers prepared food, wove camouflage nets, etc. It is worth noting that schoolchildren also actively participated in volunteer activities. And the activity of some of the schoolchildren is simply amazing. They read with admiration the news about the schoolboy who independently made a drone and handed it over to the military. Practically every Ukrainian in one way or another contributed to the assistance of the army. Someone was engaged in practical activities, for example, repairing machinery or making so-called trench candles. Some gave their own car to military units. Many people gave money for the army, doing it through large foundations or collecting on their own for certain things that specific units needed. Volunteers took food, necessary equipment and ammunition to the battle line. Volunteer activity does not stop to this day.

Only two weeks after the start of the war, stalls and some shops began to open and a more or less stable supply of goods to grocery stores began. Of course, everything depended on where exactly the stores were located, how their work was organized, etc. Of course, there were shops that did not stop their activities. In the first weeks of the war, free food aid was organized for the least well-off sections of the population. It is worth noting that at the beginning of the

war, a complete ban on the sale of alcoholic beverages was introduced. The relaxation of the ban on the sale of alcohol began after three months of hostilities. Accordingly, in the regions located west of Kyiv, the situation with the supply and operation of all life support services was better.

Despite the difficult military situation around Kyiv, life support services worked well. The apartments of the residents of Kyiv had electricity, water, and heat. Of course, there were failures, but in general the situation was acceptable. Mass media worked constantly. Of course, the number of TV channels became smaller, and those that remained united and transmitted a single information block of news. It should be noted that Internet providers also worked. Mobile communication was working. Therefore, residents of Kyiv were not cut off from the world and received operational information about events at the front. We think that the absolute majority of Ukrainians followed and continue to follow the news. Someone watches TV, someone uses the Internet, watching the news or reading messages on social networks.

Medical care in Kyiv faced serious challenges during the war. Many pharmacies have stopped their work due to lack of staff. And those who remained to work often did not have the entire range of medicines. Many polyclinics stopped their work. However, online consultation of patients by doctors was organized. At the same time, the medical facilities that remained open were forced to adapt to the new conditions, implementing emergency measures to provide medical care during shelling, interruptions in the supply of medicines and equipment, as well as evacuation processes. Kyiv hospitals did not stop their work. They became centers where they provided assistance to the wounded at the front.

Already in the first days of the war, the military administration of Kyiv and other cities and regions of Ukraine introduced a curfew. The curfew in Kyiv remains until today and lasts from 00:00 to 05:00 in the morning. At the beginning of the war, there were cases when a curfew was introduced for several days. This was done in order to fight subversive groups of Russians.

At the beginning of the war, residents of Kyiv heard the first air raid alarms. In this regard, storage facilities were restored and shelters were organized for the population. It is worth noting that it was possible to go to the shelter even during the curfew. Adapted basements of buildings, underground passages, subway stations, etc. serve as shelters. Many people spent several days in shelters, especially at the beginning of the war.

Ground transport and the subway did not work in the first weeks of the war.

4. CONTINUATION OF THE WAR AND RESTORATION OF LIFE IN KYIV

After the retreat of the Russian aggressors from Kyiv, people began to return to the city. Of course, the war continued. But the forced break in work could not last too long. For example, education workers, who were on forced leave, began to resume the work of educational institutions after only 2 weeks. Initially, this happened in the western regions of Ukraine, and gradually the educational process began to be restored throughout the territory of Ukraine, as well as in Kyiv.

Not only the improvement of the security situation, but also the cancellation of state aid, which was received by forcibly displaced persons, contributed to the return of Kyivans to their native city. At the time when the battle line passed near Kyiv, citizens evacuated from Kyiv received monetary and food aid. Help is received today by resettled people from regions with a high level of military danger. Payments of assistance for resettlement and loss of housing as a result of hostilities are regulated by the legislation of Ukraine.

A few months after the start of the Russian invasion, life in Kyiv began to improve. Businesses, shops, bazaars have resumed their work. Catering establishments, cafes and restaurants began to open. Of course, they worked with certain restrictions, which gradually weakened. For example, the ban on the sale of alcohol after certain hours was lifted only

recently. Queues in pharmacies have disappeared. The range of medicines was restored, which was critical in the conditions of the first weeks of the war, when it was not possible to buy some necessary medicines. The work of the polyclinic has been resumed. Undoubtedly, the destruction of medical institutions by the Russian aggressors led to a partial cessation of their work. For example, the remains of a Russian drone fell near a polyclinic in the Desnyan district of Kyiv. At the same time, people who wanted to enter the storage facility located in this polyclinic died. As a result, the polyclinic building is still in a damaged state and is not functioning. Doctors hold appointments in various medical centers or departments located in the same area. Undoubtedly, it was not possible to restore a full set of medical services. However, the modern system of medical care in Ukraine makes it possible to receive medical assistance in any medical institution of the country. The easiest way to do this is to use a special Internet system and the "Helsi" application.

5. LIFE IN KYIV IN MODERN CONDITIONS OF WAR

Life in Kyiv became much safer after the retreat of Russian troops. This is clearly evidenced by the resumption of activities of foreign embassies and consulates of foreign countries. Today, Ukraine is visited by presidents, prime ministers and top leaders. The improvement of the security situation contributed to the return of a significant number of Kyiv residents from evacuation. In addition, Kyiv became a refuge for forced migrants from settlements that were located near hostilities. Fewer people live in Kyiv today than before the full-scale invasion of Russian troops.

The work of enterprises resumed. State institutions, educational institutions, and cultural institutions functioned. Transport began to operate regularly. Buses, trolleybuses, trams, subways and shuttle taxis began to operate in pre-war mode.

The range of food stores has practically returned to the pre-war level. It seemed that the war had receded and the people of Kyiv began to live a normal, peaceful life. However, the impact of the war is constantly felt by the residents of Kyiv and other populated areas of Ukraine. Russia continues to carry out massive strikes with cruise missiles, ballistic missiles and combat drones on the territory of Ukraine. Not only military facilities and critical infrastructure facilities are under fire, most often civilian buildings. More than 29,000 objects were destroyed and damaged in Kyiv and the region. According to data as of April 2024, almost 17,500 objects have already been completely and partially restored with life support. In particular, more than 15,800 multi-apartment and private buildings, 202 educational institutions, 115 health care facilities, and 78 administrative buildings have already been restored (Reconstruction of Kyiv region: almost 17,500 objects were restored out of more than 29,000 damaged ones Website "Public Kyiv"). However, Russian missile attacks continue, and accordingly the number of destroyed and damaged buildings in Kyiv is increasing. On July 8, 2024, Russia delivered another powerful blow to Kyiv. In particular, the largest children's hospital, Okhmatdyt, came under attack. It wasn't Russia's mistake, it wasn't an accidental missile deflection. Thus, Russia pursues a policy of intimidation and destruction of the civilian population of Ukraine.

Missile strikes and combat drones posed and pose a real and serious danger to the residents of Kyiv, businesses, communications and critical infrastructure. Air alarms happen quite often, even several times a day. Air alarms have a dangerous psychological and physiological effect on people. Anxiety disrupts sleep. Many people do not sleep well at night, feel tired, get sick more often. Some people follow the rules and take shelter during an air raid. But a large part of Kyiv residents are very tired of constant air alarms. They stay at home. Some of them follow the "two walls" rule, but many do not change their routine. This is not due to neglect of danger, but because living by the rules in the case of an air alert turns into a constant nightmare. The Russians, knowing this, carry out false measures that are perceived as an opportunity to launch

cruise or ballistic missiles and thus worsen the psychological and physiological situation for the population of Kyiv. It is worth noting that at enterprises and institutions, safety rules are more carefully observed during an air alert. At the same time, the staff must go to the shelter. Safety rules are strictly followed in all educational institutions from preschool to higher education. Even during remote classes using online services, after the announcement of an air alert, classes are suspended and resumed after it ends. There are not rare cases when classes in schools take place in shelters during an air raid. Important meetings at enterprises and organizations can also be held in shelters. Air alarms significantly affect the ability to move around Kyiv. During an air alert, public transport stops: trolleybuses, buses, trams. The metro operates only within the underground sections. Therefore, it is extremely difficult to get from the left bank of Kyiv to the right bank or vice versa. Only taxis and shuttle taxis remain in operation. People are late for work, late for trains and long-distance buses. Even if you leave early, there is no guarantee that you will be able to make it to the required hour.

The work of trade establishments during air raids is regulated, for the most part, by internal orders. Some shops stop working during air alarms. However, some large supermarkets are open even during the emergency. This is due to the large number of customers in the premises and, accordingly, the considerable time and complexity of temporarily closing the store. At the beginning of the war, more shops practiced closing during air raids. With the increase in the frequency of alarms, as well as the improvement of air defenses around Kyiv, more and more shops continue to operate during alarms. However, if necessary, they can stop working.

In September 2024, there was no air raid alert in Kyiv only on September 1. Statistics of air alarms are published in the "Kyiv digital" system. From September 1 to 5, 8 air alarms sounded in Kyiv, the longest of which lasted 9 hours and 8 minutes (Tab. 1).

Table № 1: Air alarms in Kyiv from September 1 to 5, 2024.

Time and date	Notification of alarm or alarm rejection	Duration of the air alarm
23:45 05.09.24	🟢 Repulse of the air alarm	7 minutes
23:37 05.09.24	🔴 Air alarm!	
23:31 05.09.24	🟢 Repulse of the air alarm	20 minutes
23:11 05.09.24	🔴 Air alarm!	
12:46 05.09.24	🟢 Repulse of the air alarm	31 minutes
12:15 05.09.24	🔴 Air alarm!	
08:38 05.09.24	🟢 Repulse of the air alarm	9 hours 8 minutes
23:29 04.09.24	🔴 Air alarm!	
07:05 04.09.24	🟢 Repulse of the air alarm	4 hours 23 minutes
02:41 04.09.24	🔴 Air alarm!	
04:22 03.09.24	🟢 Repulse of the air alarm	31 minutes
03:50 03.09.24	🔴 Air alarm!	
01:26 03.09.24	🟢 Repulse of the air alarm	16 minutes
01:10 03.09.24	🔴 Air alarm!	
06:27 02.09.24	🟢 Repulse of the air alarm	1 hour 47 minutes
04:40 02.09.24	🔴 Air alarm!	

Source: History of air alarms in Kyiv as a result of Russian military aggression. Website: "Kyiv Digital"

Since February 24, 2022, a total of 1,244 alarms have sounded in the city of Kyiv. The total duration of alarms was 1,361 hours and 53 minutes, which is almost 57 full days of danger.

Some of the air alerts are issued in the event of a possible threat, in particular, in the event of MIG 31 aircraft taking off from Russian territory, which may be carriers of Kinzhal missiles. In the event of the launch of cruise and ballistic missiles in Kyiv, a state of heightened danger is declared.

For example, in August 2024, Ukrainian air defenses shot down 781 out of 916 launched Russian missiles and drones. The Russian aggressors launched 680 attack drones, of which the air defense forces of Ukraine destroyed 655. The Russian aggressors launched 182 cruise, guided, anti-aircraft and anti-radar missiles, of which they managed to destroy 117. Ballistic missiles are the most difficult to destroy, they were shot down only 9 out of 54 launched. Therefore, the danger during an air alert is often real and you need to take it into account in your daily activities.

The sounds of explosions, the shots of the air defense of the Armed Forces of Ukraine, mobile groups with machine guns to destroy drones have become a part of the daily life of the people of Kyiv.

In addition to the traditional means of announcing an air alarm: turning on sirens, in some places the sound of sirens is supplemented by a voice message. In addition, mass media, radio, television, special chats in "Telegram" and other social networks report on the threat. A special system for mobile phones has also been developed, which includes the sound of a siren and a voice message in case of danger, as well as notifies the end of the alarm. This application is convenient, especially if you need to constantly monitor the threat. In particular, it is very useful in the education system, because it allows you to quickly find your way around. Stop classes and go to shelter for all participants of the educational process.

Russian aggressors launch missile strikes and drone strikes against any objects, military, houses, cultural monuments and critical infrastructure objects. Let's touch only on the energy industry. The issue that is the most painful for the population of Ukraine and Kyiv in particular. A series of attacks by Russians on energy facilities, in particular, on thermal power plants and hydroelectric power plants, disrupted the normal activity of the energy industry. Ukrainians, and in particular, residents of Kyiv, have already experienced several blackouts. The insufficient amount of electricity in the energy system of Ukraine forces consumers to be temporarily disconnected from the power supply. Only critical infrastructure facilities, hospitals, etc., receive energy continuously. Life in conditions of constant power outages is quite difficult. In the journalistic aspect, it could be called "Life to the sound of generators". Indeed, to solve the issue of power supply, many small and large enterprises, pharmacies, shops, supermarkets, etc., have purchased gasoline and diesel generators. In the event of a power outage, businesses and individual residents turn on generators. Of course, generators make noise, which is why the phrase "Living to the Noise of Generators" was coined. The purchase of generators partially solves the problem of the work of large or small enterprises. The population most often buys batteries, uninterruptible power supply stations, small solar batteries that are installed on the balconies of apartment buildings.

A lot depends on electricity. Not only the light in the houses, but also the operation of mobile phones and mobile networks, telecommunication lines and the Internet. Today, Internet service providers are starting to use equipment more and more, in particular, signal transmission over fiber optic cables, which allows you to get the Internet even in the event of a power outage. The user usually only needs to ensure the connection of a small uninterruptible power supply to the block of the Internet provider and the modem. However, powerful batteries and inverters are required for full energy supply. Therefore, most residents of Kyiv have problems with the functioning of household appliances, in particular, refrigerators, electric stoves, etc. Not

everyone has the financial ability to purchase an uninterruptible power supply or to assemble a system from a battery, inverter and charger with their own hands.

Power outages force a number of enterprises to temporarily stop working, which has an extremely bad effect on the economic situation.

For example, let's present the educational sector. Generators are available today in many educational institutions, schools, universities, etc. But these generators cannot ensure the full functioning of the educational institution. Computers, interactive whiteboards and other equipment do not work. Most often, the main task of using generators in educational institutions is to illuminate shelters during air alarms and during simultaneous power outages. Each educational institution solves the problems of electricity supply independently. During the day without electricity, you can conduct face-to-face classes. However, many lessons, trainings and other activities take place remotely. The first difficulty. It is practically impossible to predict the time of power outage for more than a day. Therefore, there are difficulties with planning and constant postponements of classes. The second difficulty. In different districts of Kyiv, blackouts occur according to their own schedules, so it is impossible to choose a time when all recipients of educational services have electricity and, accordingly, an Internet connection.

To solve the issue of electricity supply and communication, a network of so-called "Points of Invincibility" has been deployed in Kyiv. These points are equipped with generators, and in winter - with heaters. At the unbreakable point, you can charge your mobile phone or laptop, or even listen to a lesson or training. However, it is difficult to conduct classes on the point of indomitability, because there are usually other people there. Real cases of holding classes on points of indomitability were written about in Kyiv news.

In addition to power outages, water and heat supply systems may be damaged or even destroyed as a result of missile strikes and the use of drones. There were such cases in Kyiv, but thanks to the prompt work of the repair crews, the damage can be repaired more or less quickly. However, the residents of Kyiv are anxiously awaiting the cooling period and the onset of frost. The past war winters showed that the temperature in the houses was lower compared to the temperature in peacetime. Cold in homes, educational institutions, and enterprises does not contribute to efficient work and negatively affects people's health. Especially vulnerable to low temperatures are children, the elderly and people with weakened health, which creates an additional burden on the health care system in wartime conditions.

CONCLUSION

Life in Kyiv during the war is characterized by a number of dangers. Direct military hazards are created during the use of weapons. Indirect military dangers are associated with the complete or partial shutdown of enterprises and transport during air strikes, blackouts of electricity, communications, heat and water supply. The evacuation of Kyiv residents led to a shortage of labor resources and reduced the efficiency of enterprises. All this has a negative impact on the economy of the country and on the psycho-emotional and physical condition of the residents of Kyiv.

However, the absolute majority of Kyivans are trying to cope with war risks. They work as volunteers, allocate their own funds for the purchase of this or that equipment for the Armed Forces of Ukraine. Practically every Ukrainian directly or indirectly participates in the war. A country where everyone is ready to fight is invincible!

REFERENCES AND INFORMATION SOURCES

1. Відбудова Київщини: відновлені майже 17,5 тис. об'єктів із понад 29 тис. Пошкоджених Сайт «Суспільне Київ», 2024 (Reconstruction of Kyiv region: almost

17,500 objects were restored out of more than 29,000 damaged ones Website "Public Kyiv", 2024) URL: https:// https://suspilne.media/kyiv/728361-vidbudova-kiivsini-vidnovleni-majze-175-tis-obektiv-iz-ponad-29-tis-poskodzenih/

2. Історія повітряних тривог у Києві внаслідок російської військової агресії. Сайт: «Kyiv Digital». 2024. (History of air alarms in Kyiv as a result of Russian military aggression. Website: "Kyiv Digital". 2024.) URL: https://kyiv.digital/storage/air-alert/stats.html

CONTACT INFORMATION

Hon. Professor, docent Vasyl ZAPLATYNSKYI CSc.
Department of Natural and Mathematical Education and Technologies,
Borys Grinchenko Kyiv Metropolitan University;
Academy of Safety and Bases of Health
st. Milyutenko 17, fl. 67, s. Kyiv, 02156,
Ukraine
vasyl.zaplatynskyi@gmail.com
ORCID iD – 0000-0003-0119-7135

Docent. Ing. Inga URIADNIKOVA CSc.
Department of water supply and drainage
Kyiv National University of Construction and Architecture,;
Academy of Safety and Bases of Health
st. Milyutenko 17, fl. 67, s. Kyiv, 02156,
Ukraine
ingavictory@gmail.com
ORCID iD – 0000-0002-3750-876X

The College of European and Regional Studies
Department of Law and Security Studies

INTERNATIONAL CONFERENCE SAFE AND SECURE SOCIETY 2024

Edited by
Štěpán Kavan

Publisher:
The College of European and Regional Studies
Žižkova tř. 1632/5b, České Budějovice
Czech Republic, 2024
www.icsss.eu

https://doi.org/10.36682//SSS_2024
ISBN 978-80-7556-151-0
ISSN 2533-6223