Vol. 9 No. 2 (2025)
ISSN 3072-1717

Akademia WSB
WSB University

SECURITY FORUM

TERRITORIAL DEFENCE FORCES AND CONTINUITY OF ACTION IN COMBATING NATURAL DISASTERS

CYBERSECURITY AS A KEY ELEMENT OF NATIONAL SECURITY: AN ANALYSIS OF THREATS AND DEFENSE STRATEGIES IN THE 21st CENTURY

SAFETY AT THE SHOOTING RANGE DURING FIREARMS TRAINING PROTECTION OF THE LOCAL POPULATION AND RISK MINIMIZATION

SECURITY
FORUM

Work on the development of the edition has been completed: December, 2025

ISSN 3072-1717

Editorial Board:

WSB University

SECURITY FORUM

Vol. 9 • No. 2 (2025)

SEMIANNUAL JOURNAL

Published by WSB University

CONTENTS

CYBER SECURITY

SECURITY LAW

SECURITY – CASE STUDIES

MISCELANEA

PREFACE

My professional and academic interests for many years have focused on new technologies and security. I work within the ranks of the State Fire Service (PSP), where I handle both the certification and approval of fire service equipment and apparatus, as well as the certification of construction products used in fire protection. Additionally, I conduct scientific research in fire safety, including the safety of new technologies. For many years, the PSP research institute – the Scientific and Research Centre for Fire Protection – PIB- has provided a platform for me to not only fulfil my official duties but also pursue my passions related to the safety of rescuers, victims, equipment, firefighting systems, and passive fire protection measures in buildings. Scientific research into safety enables better implementation of new technologies in practice and more effective achievement of protection objectives. Rapid technological progress has intensified challenges and needs in this field, especially recently. The safety of new technologies is crucial for their practical application. To ensure safety, research must be conducted, results thoroughly analysed, various perspectives considered, real threats identified, assessed, and appropriate measures adopted to minimise or mitigate risks. Although my activities and considerations are primarily related to fire safety, the scientific research, qualification studies, and knowledge I gain are valuable in the broader context of understanding safety.

It is therefore not surprising that both scientists and practitioners are interested in the results of scientific research and the considerations based on them. It appears that the biannual Security Forum published by WSB University is a highly respected journal that combines the achievements of security sciences with political and administrative sciences, addressing the professional needs and

interests of practitioners and implementers from various fields and disciplines, both scientific and professional. What unites these different environments is the fact that the scientific articles, conclusions, and materials published in Security Forum are original work by specialists in specific fields of knowledge, covering various aspects of security. Consequently, the journal serves as an excellent source of both scientific knowledge and inspiration for practical applications and activities within the broadly understood field of security

st. bryg. dr hab. inż. Jacek Zboina
Deputy Director for Certification and Approvals
Józef Tuliszkowski Fire Protection Research Centre

António Tavares, PhD
Lusófona University of Porto
e-mail: p4471@ulp.pt
ORCID:0000-0003-3222-727X

Wiktoria Kolano, MA
WSB University in Dąbrowa Górnicza
e-mail: wkolano@wsb.edu.pl
ORCID:0000-0003-3047-8622

DOI: 10.26410/SF_2/25/1

ENERGY TRANSITION AND INTERNATIONAL SECURITY: THE ROLE OF THE EUROPEAN UNION AND NATO IN BUILDING RESILIENCE TO GEOPOLITICAL THREATS

Abstract

This article analyses the impact of the energy transition on international security, with a focus on the actions of the European Union and NATO. It discusses mechanisms for supply diversification, the development of renewable energy sources, the protection of critical infrastructure and the threats posed by raw material dependence. The strategic importance of synergies between energy policy and security is highlighted, pointing to the growing role of transatlantic cooperation in building resilience to geopolitical threats.

Keywords

Energy security, critical infrastructure, strategic resilience, geopolitical threats, energy supply diversification

Introduction

In the context of deepening competition for strategic resources and a redefinition of the international order, the energy transition is becoming not only political and economic, but also geostrategic. Changing paradigms of energy production and consumption are determining new lines of division, alliances and tensions, redefining the classical notion of state security. In this dimension, energy policy is no longer the domain of technocratic strategies – it is becoming a field where the interests of states, international organisations and supranational actors clash.

The growing importance of renewable energy sources and the raw materials necessary for their development, such as lithium, cobalt or rare earths, highlights a new form of dependency, this time oriented around so-called 'green supply chains'. Their control is becoming the subject of an intense geopolitical game, in which the advantage is not necessarily gained by the largest CO_2 emitters, but by those who can effectively manage access to the technology, know-how and raw materials necessary for the transformation.

In the face of these challenges, the EU and NATO are increasingly integrating energy issues into their strategic priorities, treating it as a foundation for systemic resilience and community political cohesion. The answer to the question of how energy policy translates into the ability to respond to hybrid threats, destabilisation of border regions or commodity pressures from authoritarian actors is becoming crucial for the future of the European and transatlantic security architecture.

This article attempts to identify and interpret these relationships in the context of current geopolitical processes, with a particular focus on the mechanisms implemented by the European Union and NATO. The analysis is based on the conviction that the energy transition is not an isolated phenomenon, but deeply embedded in the structure of contemporary international relations – becoming one of the key tools for redefining the global balance of power in the 21st century.

Methodological and methodical assumptions

The aim of this article is to analyse in detail the mechanisms and strategies adopted by the EU and NATO to strengthen resilience to the geopolitical threats accompanying the energy transition and to assess the impact of these actions on international security. The research question posed is how the mechanisms developed and strategies implemented enhance international stability and the effectiveness of these organisations' responses to contemporary energy challenges. The study is based on an analysis of the literature on the subject, normative documents and statistical data, as well as historical and contemporary determinants of energy security policy. The methodology of the study includes a critical analysis of sources, a comparison of mechanisms and an assessment of their effectiveness in the context of current geopolitical developments. The analysis conducted allows for the identification of key

challenges and the definition of the role of these organisations in the global energy transition process. The structure of the article is designed to provide a holistic view of the issue – from an introduction to basic concepts and the embedding of the energy transition in the context of international security, to an analysis of specific strategies and mechanisms implemented by the EU and NATO. The different parts of the text cover both the strategic and operational perspectives of the measures taken.

Energy transition as an element of international security

Energy transition is one of the key elements of contemporary international security, as it reduces dependence on imported energy resources while diversifying supply. The European Union imported 90% of its natural gas by 2022, with as much as 45% coming from Russia.

This situation highlighted the strategic risks associated with such significant dependence on a single supplier. In response to these challenges, the implementation of the energy union was launched, including the construction of the LNG terminal in Swinoujscie, which plays a key role in reducing the EU's energy dependence. This terminal is capable of receiving units of up to 150,000 m^3 and regasification allows the volume of liquefied gas to be increased to around 600 m^3 of mains gas. The importance of this infrastructure goes beyond the borders of Poland, also strengthening the energy security of the entire EU[1]. One of the priorities within the energy transition strategy is the diversification of supply and the construction of energy rings, which include cooperation with Germany, Sweden and Lithuania. Such measures counteract the geopolitical risks arising from the dominance of a single supplier. The development of renewable energy is another important aspect that fits into the strategy of strengthening international security. In 2021, renewable energy accounted for 21.8 per cent of EU energy consumption, showing a growing trend towards decarbonisation. These actions highlight the EU's role as a leader in the fight against the climate crisis and strengthen the geopolitical stability of the region[2]. The international impact of the energy transition can also be seen in the reduction of greenhouse gas emissions. In the EU, these emissions have decreased by 31% between 1990 and 2020, demonstrating the effectiveness of climate strategies.

Reducing emissions not only contributes to environmental protection, but also minimises conflicts over resources of traditional energy resources[3]. Investment in renewable energy sources positively impacts the global perception of the region as a leader in environmental action and promotes international stability[4]. However, the

1 T. Jerzyniak, *The EU De-Risking of Energy Dependencies: Towards a New Clean Energy Geopolitical Order? Politics and Governance*, 2024, p. 4.

2 P. Mickiewicz, *Determinants of the maritime security strategy of the Republic of Poland, Yearbook of Maritime Security*, 2013, VII, p. 302.

3 A. Pinkas, *Climate protection as a determinant of energy system integration*, Folia Iuridica Universitatis Wratislaviensis, 2022 11(2), p. 19.

4 A. Widuto, *Energy transition in the EU,* European Parliamentary Research Service, PE 754.623, Brussels 2023, p. 3.

challenges of the energy transition cannot be overlooked. The EU is highly dependent on imports of critical minerals such as lithium, cobalt and rare earths, 90% of which come from China. Forecasts indicate that demand for these minerals will triple by 2030 under a net zero emissions scenario. Such a situation poses not only a technical challenge, but also a strategic one, forcing the EU to develop a strategy to diversify its supply and establish international cooperation in order to reduce the risks arising from China's dominance[5]. The construction of critical infrastructure, including the LNG terminal in Swinoujscie, is one of the EU's key actions to ensure energy security. Such investments strengthen the reliability of gas supply and increase the region's energy resilience. The EU additionally plans to step up investment in energy infrastructure to €530 billion per year by 2030. This reflects a commitment to long-term energy plans, which also require extensive international cooperation[6]. The development of modern technologies, such as hydrogen, is an important part of the region's independence from fossil fuels. The EU's hydrogen strategy aims to produce and import 20 million tonnes of hydrogen by 2030, strengthening its position in the global energy market[7]. The energy transition is also changing the global balance of power, reducing the importance of traditional energy commodities such as coal. For example, the share of coal in China's energy mix has fallen from 72.2% in 2000 to 60.4% in 2017, illustrating the global transformation of the energy sector[8]. Poland's energy policy also recognises the importance of natural gas as a key component of the energy transition. Burning natural gas produces almost twice as much carbon dioxide compared to oil or coal, making it a greener transition fuel. In 2005, Poland's natural gas production amounted to 4.3 bcm and allowed it to cover about 31% of the domestic demand for this fuel, which underlines the importance of domestic resources in ensuring energy security. It is also worth noting the projected global growth in natural gas consumption of 2.3% per annum, from 2442 bcm per annum in 2000 to a projected 4831 bcm per annum in 2030, illustrating the growing role of this resource in the global energy mix[9]. NATO also recognises the importance of the energy transition in the context of international security. As part of the NATO 2030 programme, the organisation is focusing on diversifying supply chains, protecting critical infrastructure and countering hybrid threats such as cyber attacks and disinformation. Intensive international cooperation, including joint monitoring and harmonisation of operations, is key to effectively countering such threats. NATO initiatives raise awareness of energy threats and strengthen the Alliance's position as

5 T. Jerzyniak, *The EU De-Risking of Energy Dependencies: Towards a New Clean Energy Geopolitical Order? Politics and Governance*, 2024, p. 4.

6 J. Trubalska, *Energy Union – a key concept in EU energy policy,* Pulaski Policy Papers, 2015, p. 1.

7 A. Widuto, *Energy transition in the EU,* European Parliamentary Research Service*, PE 754.623,* Brussels, 2023, p. 5.

8 A. Wilgos, *The importance of the renewable energy sector in building China's energy security*, Doctoral dissertation, Poznań University of Economics, 2018, p. 3.

9 S. Rychlicki, J. Siemek, *Natural gas in the energy policy of Poland and the European Union. Energy Policy*, 2008 11(1), pp. 2-3, 9.

a key actor in the security area[10]. In summary, energy transition is a multidimensional process that not only contributes to strengthening international security, but also changes geopolitical dynamics on a global scale. Actions at EU and NATO level reflect the strategic importance of this transition in both regional and global contexts.

Mechanisms for building resilience to geopolitical threats

Diversification of energy sources is a key element of a strategy to increase resilience to geopolitical threats[11]. An example of such efforts is the development of LNG infrastructure, including the Swinoujscie terminal, which allows for the regasification of liquefied natural gas up to 600 m^3 per LNG unit. This type of investment reduces dependence on a single supplier, such as Russia, which supplied the European Union with 45% of its natural gas needs before 2022. As a result, the development of such projects not only strengthens energy security, but also enables a more flexible response to crises[12]. As part of the NATO 2030 programme, extensive activities have been undertaken to protect and diversify energy supply chains.

Key activities include the identification of gaps in critical infrastructure and the intensification of joint initiatives between Alliance member states. In the face of geopolitical threats, such as potential energy supply disruptions, NATO is also increasing its commitment to promoting cooperation and monitoring potential threats in real time, an important step in building resilience[13]. Diversification of energy sources is also a key element of the European Union's climate policy. Investments in the renewable energy sector and the development of new technologies, such as green hydrogen production, are aimed at reducing greenhouse gas emissions and reducing dependence on fossil fuels. These activities not only support a sustainable energy transition, but also contribute to reducing geopolitical risks arising from the dominance of traditional raw material suppliers[14]. Monitoring private sector activities plays an important role in minimising losses from energy risks. The example of Indonesia, where the private sector is engaging in infrastructure investment, demonstrates the importance of publicprivate sector partnerships in ensuring energy stability. Such cooperation can also inspire other regions that face similar energy security challenges[15]. Investment in the development of critical infrastructure, including renewable energy sources and hydrogen technologies, is the foundation for building stability of energy supply. The European Union's strategy is to produce 10 million tonnes of

10 T. Nowak, *Building resilience to current and future hybrid threats, Roczniki Nauk Społecznych*, 2022 14(50)(4), p. 31, 37.

11 P. Mickiewicz, *Determinants of the maritime security strategy of the Republic of Poland, Yearbook of Maritime Security*, 2013, VII, p. 302.

12 T. Jerzyniak, *The EU De-Risking of Energy Dependencies: Towards a New Clean Energy Geopolitical Order? Politics and Governance*, 2024, p. 4.

13 T. Nowak, *Building resilience to current and future hybrid threats, Annals of Social Science*, 2022 14(50)(4), p. 31.

14 A. Widuto, *Energy transition in the EU,* European Parliamentary Research *Service, PE 754.623,* Brussels, 2023, p. 5.

15 M. Telus, *Quality of education in higher education with particular reference to non-public schools in Poland, Economy and Finance*, 2018 Zeszyt 9, p. 91.

hydrogen and import the same amount by 2030. This is a significant step towards the decarbonisation of the economy, which at the same time reduces the geopolitical risks arising from dependence on fossil raw materials[16]. Having an adequately developed infrastructure, such as the LNG terminal in Swinoujscie, is key to responding quickly and effectively to energy crises. An infrastructure base of this type is fundamental to national and regional strategies for building resilience to threats. The example of Poland shows that investments in energy infrastructure can significantly strengthen security at both national and international levels[17]. Modernising and securing key energy infrastructure requires significant financial investment. The European Union is planning investments of €530 billion per year until 2030 to meet the challenges of the energy transition. Securing adequate financial resources and using them efficiently is key to achieving security and energy stability objectives[18]. The experience of infrastructure management in the education and science sector can be a valuable resource for the energy sector. Diagnosing problems such as outdated structures or financial shortfalls allows better management of transformation processes in other sectors. Cooperation between different fields of knowledge can bring innovative solutions to global energy challenges[19]. Transatlantic cooperation within NATO plays an important role in countering cyber attacks and disinformation that affect the security of critical infrastructure. Monitoring threats and developing strategies to respond to adversaries' hybrid activities are crucial for NATO member states. Such projects strengthen the alliance's cohesion and highlight its role in building international security[20]. The integration of energy policy with security policy within the EU and NATO contributes to strengthening resilience to energy disruptions. Examples of joint initiatives, such as conflict monitoring and taking stabilisation measures in sensitive regions, demonstrate the importance of a synergistic approach between the two domains. Effective international cooperation minimises risks and generates new opportunities in the face of global challenges[21]. Harmonisation of technological and regulatory standards through transatlantic cooperation supports the development of common defence mechanisms. These initiatives enable countries to create a unified framework for dealing with energy threats, which is crucial for the coherence of security strategies[22]. Considering the impact of migration on the strain on energy resources is important in the context of humanitarian crises. During the 2022 refugee crisis, it was noted how important it is to coordinate actions in the area

16 T. Jerzyniak, *The EU De-Risking of Energy Dependencies: Towards a New Clean Energy Geopolitical Order? Politics and Governance*, 2024, p. 4.

17 P. Mickiewicz, *Determinants of the maritime security strategy of the Republic of Poland. Maritime Security Yearbook*, 2013, VII, p. 302.

18 A. Widuto, *Energy transition in the EU,* European Parliamentary Research Service*, PE 754.623,* Brussels, 2023, p. 6.

19 M. Telus, *Quality of education in higher education with particular reference to non-public schools in Poland, Economy and Finance*, 2018 Zeszyt 9, p. 189.

20 T. Nowak, *Building resilience to current and future hybrid threats, Roczniki Nauk Społecznych*, 2022 14(50)(4), p. 37.

21 E. Bendyk, P. Buras, *Poland in the face of war, Poland in the post-war world*, Stefan Batory Foundation, 2022, pp. 1-3.

22 T. Nowak, *Building resilience to current and future hybrid threats, Roczniki Nauk Społecznych*, 2022 14(50)(4), p. 37.

of both social and energy infrastructure. The examples of countries such as Hungary and Romania point to the contribution of international cooperation to maintaining socio-economic stability[23]. European Union regulations, such as directives on energy security, support the energy transition and the development of renewable energy sources. The increase of the RES share in the EU energy mix to 38% in 2020 confirms the effectiveness of these regulations. Further development of legislation in this area is necessary to meet future challenges[24]. The EU's critical minerals policy requires strategic changes to diversify supply and reduce dependence on China. Projections indicating a threefold increase in demand for these minerals by 2030 highlight the importance of precise legal provisions that could secure mineral supplies and minimise geopolitical risks[25]. Securing financing and developing mechanisms to support investment in renewables is one of the cornerstones of increasing resilience to energy supply disruptions.

Stable financing of energy projects enables the EU to meet its climate and economic targets[26]. Think tanks, such as the Pulaski Foundation, provide invaluable analysis and recommendations to support precise energy policy planning. The influence of experts in defining strategic priorities contributes to more effective implementation of transformational programmes, as noted in research on international security[27]. The integration of electricity systems between non-EU countries, as in the case of Ukraine in 2022, strengthens regional energy stability. Such initiatives reduce the effects of armed conflicts on regional energy security, while promoting further international cooperation[28]. Regional projects such as the Baltic Pipe or cooperation within the Tri-Community are an important element in strengthening the geopolitical position of Central and Eastern Europe. They reduce the region's dependence on global suppliers of energy resources, while contributing to increased stability and security[29]. The development of defence capabilities in Central and Eastern Europe is essential in the face of growing hybrid threats, including destabilising actions by Russia. Investment in regional defence mechanisms strengthens energy resilience and overall national security[30]. Countries such as Hungary and Romania, which are supporting Ukrainian refugees, point to the benefits of international crisis cooperation. Integrating action during humanitarian crises affects the socio-economic

23 A. L. Dumitrescu, V. Consta*NTIN, The Socio-Economic Impact of Migration in the EU: In the Case of Ukraine Refugees.* Centre for European Studies Department, Institute for World Economy, Ministry of Internal Affairs, 2022, p. 10.

24 J. Pepe, *Geopolitics and Energy Security in Europe*, Friedrich-Ebert-Stiftung, 2022, p. 7.

25 T. Jerzyniak, *The EU De-Risking of Energy Dependencies: Towards a New Clean Energy Geopolitical Order? Politics and Governance*, 2024, p. 4.

26 A. Widuto, *Energy transition in the EU,* European Parliamentary Research Service*, PE 754.623,* Brussels, 2023, p. 5.

27 T. Pawłuszko, *International security in the research of Polish think tanks. Yearbook of International Security*, 2014 8(2), p. 2.

28 E. Bendyk, P. Buras, *Poland in the face of war, Poland in the world after the war,* Stefan Batory Foundation, 2022, p. 4.

29 T. Nowak, *Building resilience to current and future hybrid threats, Roczniki Nauk Społecznych,* 2022 14(50)(4), p. 30.

30 I. Jankowska, Energy security in the state security policy, PWSZ IPIA Lubuskie Studies, 2015 Volume XI, p. 5.

stability of the region and can inspire future policies[31]. Promoting sustainable development through climate targets is another important step towards strengthening energy security. Reducing greenhouse gas emissions and reducing dependence on fossil fuels brings the European Union closer to achieving its strategic goals for the energy transition[32]. Raising the target for the share of renewables in the EU's energy mix to 40% by 2030 sets an ambitious direction for future action in energy policy. Such decisions accelerate the energy transition while minimising the economic risks arising from dependence on energy imports[33]. Flexibility in energy policy is essential in the face of global energy market shocks. Investment in low-carbon technologies, such as green hydrogen, enables the European Union to adapt quickly to changing geopolitical conditions and also increases its resilience to such challenges[34]. The support of regional cooperation and think tanks, such as the Pulaski Foundation, demonstrates the value of experts in harmonising energy policy. Their analyses and recommendations contribute to building more coherent and effective strategies at the international level[35]. In summary, comprehensive efforts to build energy resilience, including investment in RES, protection of critical infrastructure, international cooperation and diversification of energy supply sources, underpin effective energy security policies and strengthen the ability of states and international organisations to respond to contemporary geopolitical threats.

Summary

The aim of this article was to analyse the mechanisms and strategies implemented by the European Union and NATO in the context of the energy transition and its impact on international security. The considerations presented focused on showing the multidimensionality of the energy transition process and its strategic importance in the dynamically changing geopolitical realities. Issues of energy dependence, the growing importance of renewable energy sources, the challenges of critical minerals and the role of international organisations in building resilience to geopolitical threats were addressed. The analysis has shown that energy transition not only strengthens energy security, but also contributes to international stability by reducing the risk of conflict and limiting the influence of dominant states in traditional energy sectors. The results presented indicate that the aim of the thesis has been achieved and that the research questions posed have been addressed in detail. Energy transition is a key

31 A. Dumitrescu, V. Consta*NTIN*, *The Socio-Economic Impact of Migration in the EU: In the Case of Ukraine Refugees*, Centre for European Studies Department, Institute for World, Economy, Ministry of Internal Affairs, 2022, p. 11.

32 B. Fortunski, *Global justice and the energy policy of the European Union*. In O. Janikowska & J. Słodczyk (eds.), *Global justice*, University of Opole Publishing House, 2016, p. 9.

33 J. Pepe, *Geopolitics and Energy Security in Europe*, Friedrich-Ebert-Stiftung, 2022, p. 7.

34 A. Cherp, J. Jewell, *Energy security assessment framework and three case-studies*, In H. Dryer, & M. J. Trombetta (eds.), *International Energy Security Handbook*, Edward Elgar Publishing, 2013, p. 12.

35 T. Pawłuszko, *International security in the research of Polish think tanks, International Security Yearbook*, 2014 8(2), p. 13.

element of the European Union's security policy, as evidenced by measures such as the development of energy infrastructure, investment in renewable energy sources and the promotion of low-carbon technologies. The implementation of projects such as the LNG terminal in Świnoujście has significantly reduced regional dependence on a single supplier, which is a fundamental step in building resilience to geopolitical threats. At the same time, the dynamic development of renewable energy contributes to the decarbonisation of the economy, highlighting the role of the EU as a leader in green action on the international stage. In this context, the energy transition not only improves the region's energy stability, but also shapes the image of the EU as a key actor in the fight against the climate crisis. One important conclusion of the analysis is the noticeable reduction in dependence on traditional raw material suppliers such as Russia, which has significantly influenced the geopolitical balance of power. Diversification of energy sources and investments in critical infrastructure, such as the Baltic Pipe, further reduce the dominance of countries such as Russia and strengthen the position of Central and Eastern Europe on the global energy map. At the same time, the North Atlantic Alliance, as part of the NATO 2030 initiative, is focusing on protecting critical infrastructure, countering hybrid threats and fostering transatlantic cooperation, all of which contribute to an increased level of international security in the energy context. While NATO has so far been seen mainly as a military alliance, it is now playing an increasingly important role in countering energy-related threats, thus making a significant contribution to the issue at hand. The challenges identified in the article, related to the growing demand for critical minerals such as lithium or cobalt and their monopolistic control by China, highlight the need to develop European raw material strategies. The projected threefold increase in demand for these raw materials forces the EU to develop diversification policies and intensify cooperation with other regions of the world. These issues point to the need to further strengthen efforts to secure access to critical minerals, which are becoming the cornerstone of the energy transition towards green energy. Similarly, the importance of hydrogen technologies was highlighted as a promising solution for decarbonisation and decoupling from fossil fuels, further enhancing the region's energy sustainability. The analysis of the results in the context of existing research shows consistency with previous studies on the importance of reducing greenhouse gas emissions and increasing the share of RES in the energy mix. However, unlike many previous publications, this paper considers the role of NATO in building energy resilience, which brings a new perspective to the existing literature. The threads taken up in the paper on the integration of energy policy with security policy at the regional and transatlantic level provide a better understanding of the interdependencies between these domains. The findings show that the energy transition, despite its challenges, has been effective in stabilising the international situation, demonstrating the effectiveness of actions taken by both the European Union and NATO. Some limitations were highlighted during the development of the article, such as the limited availability of up-to-date figures on the impact of recent NATO and EU

actions on global energy security. Some conclusions were based on forecasts, which makes them susceptible to future volatility due to dynamically changing geopolitical circumstances.

In addition, the article focuses mainly on the actions of the EU and NATO, which may overlook the potential contributions of other international actors. All these aspects suggest the need for further research that could deepen the analysis of the role of other international organisations and countries outside the discussed structures in the energy transition process. In the long term, it would also be advisable to study the effects of the energy transition on the balance of power in the international system and the role of cross-sectoral cooperation in overcoming energy security challenges. It would be particularly important to develop an analysis of the growing demand for critical minerals and its impact on global power balances, as well as to explore the effectiveness of EU and NATO cooperation in countering hybrid threats. Further exploration of these issues will help to develop a more comprehensive vision of the energy transition as a tool not only to reduce emissions and combat the climate crisis, but also to strengthen international security.

Bibliography

Bendyk, E., Buras, P., *Poland in the face of war. Poland in the post-war world*, Expert Report of the Stefan Batory Foundation, Warsaw 2022.

Cherp, A., Jewell, J., *Energy security assessment framework and three case-studies*, Dryer, W., Trombetta, M. (Eds.), *International Energy Security Handbook*, Edward Elgar Publishing, Lund 2013.

Dumitrescu, A., Constantin, V., *The Socio-Economic Impact of Migration in the EU: In the Case of Ukraine Refugees*, Centre for European Studies Department, Institute for World Economy, Ministry of Internal Affairs, *Global Economic Observer*, 2022 vol. 10 (1).

Fortuński, B., *Global justice and the energy policy of the European Union*, [in:] *Global justice*, eds. Janikowska, W., Słodczyk, J., Opole University Publishing, Opole 2016.

Jankowska, I., *Energy security in the state security policy*, PWSZ IPIA *Lubuskie Studies*, 2015 Volume XI.

Jerzyniak, T., *The EU De-Risking of Energy Dependencies: Towards a New Clean Energy Geopolitical Order? Politics and Governance*, 2024 vol.12.

Kolano W., Tavares A., Aniołek J., *Energy security in the light of amendments to the national energy law*, *Security Forum* 2024, vol. 8. no.1.

Mickiewicz, P., *Determinants of the maritime security strategy of the Republic of Poland*, *Maritime Security Yearbook*, 2013 VII.

Nowak, T., *Building resilience to current and future hybrid threats*, *Roczniki Nauk Społecznych*, 2022 14(50)(4).

Pawłuszko, T., *International security in the research of Polish think tanks*, *Yearbook of International Security*, 2014 8(2).

Pepe, J., *Geopolitics and Energy Security in Europe*, Friedrich-Ebert-Stiftung Foundation Expert Report: Brussels 2022.

Pinkas, A., *Climate protection as a determinant of energy system integration*, *Folia Iuridica Universitatis Wratislaviensis*, 2022 11(2).

Rychlicki, S., Siemek, J., *Natural gas in the energy policy of Poland and the European Union*, *Energy Policy*, 2008 11(1).

Socha, R., Kolano, W. (eds), *Challenges for State Security in the Third Decade of the 21st Century*, AWSB, Dąbrowa Górnicza 2021.

Telus, M., *Quality of education in higher education with particular reference to non-public schools in Poland*, *Economy and Finance*, 2018 (9).

Trubalska, J., *Energy Union – a key concept in EU energy policy*, *Pulaski Policy Papers*, 2015 No. 1(15).

Widuto, A., *Energy transition in the EU*, European Parliamentary Research Service, PE 754.623, Brussels 2023.

Wilgos, A., *The importance of the renewable energy sector in building China's energy security*, Doctoral dissertation, Poznań University of Economics, Poznań 2018.

About the Authors

António Tavares, PhD, Professor at Lusófona University. Director of First-cycle Political Science and Electoral Studies. Director of Second-cycle International Relations studies at Lusófona University. He is an expert in the fields of legal, political, and security sciences.

Wiktoria Kolano, Academic staff member in the Department of Security Studies at WSB University, Deputy Director of the Academic Center for Education about Auschwitz and the Holocaust at WSB University, and PhD candidate. Her research interests include, among others, comparative analyses of the organization and functioning of national security sectors, with a particular focus on Poland and Portugal.

Grzegorz Piątkiewicz, PhD
Jan Długosz University in Częstochowa
e-mail: g.piatkiewicz@ujd.edu.pl
ORCID: 0000-0001-7045-0902

DOI: 10.26410/SF_2/25/2

TERRITORIAL DEFENCE FORCES AND CONTINUITY OF ACTION IN COMBATING NATURAL DISASTERS

Abstract

The article presents the role and importance of the Territorial Defence Forces (WOT) in the crisis management system of the Republic of Poland, with particular emphasis on counteracting and responding to natural disasters. Since taking over responsibility for the non-military part of crisis management tasks in the Ministry of National Defence under the Homeland Defence Act, the WOT has become a key component of the Armed Forces in this area. The author presents the evolution of the formation, its structure and tasks, emphasising that the effectiveness of the WOT has been confirmed in a number of operations, such as support for actions during the COVID-19 pandemic, the crisis on the Polish-Belarusian border, and especially during Operation Phoenix after the floods in 2024.

The results of a survey conducted among students confirmed the positive image of the WOT and the high assessment of the effectiveness of its activities, which, according to the respondents, justifies its systematic development. a comparative analysis with the European Union's crisis response system points to its mainly coordinating nature and the lack of permanent executive forces, which highlights the value of Poland having an integrated formation such as the WOT. China's actions during the so-called "winter of the millennium" in 2008 were cited as an inspiring example of the effective mobilisation of state resources in the face of a natural disaster.

Keywords

National Security, Territorial Defence Forces, European Union, Crisis Management

Introduction

With the entry into force of the Homeland Defence Act[1], the Territorial Defence Forces (WOT) took over responsibility for the non-military part of crisis management tasks in the Ministry of National Defence[2]. WOT commanders were entrusted with the function of Head of the Ministry of National Defence Crisis Management Centre, while territorial defence brigade commanders replaced the existing heads of provincial military staffs in the field of crisis management and became the "right hand" of provincial governors in coordinating and implementing the support that the military can provide in times of crisis. These regulations have significantly strengthened the role of the WOT in building and maintaining social security.

Crisis management, as W. Kitler points out, is a significant part of state governance, focused on utilising the full potential of the nation and its allied commitments to counter threats to national security[3]. In this context, the WOT has become a key element of the crisis management system, as confirmed by operational experience: support for the police and health services during the COVID-19 pandemic, support for the Border Guard in the crisis on the Polish-Belarusian border and assistance to refugees on the Polish-Ukrainian border, as well as participation in the clean-up after the floods that affected south-western Poland in October 2024.

The main task of the WOT remains to maintain a constant state of readiness to defend the Republic of Poland through the proper preparation, training and maintenance of readiness of soldiers serving in a rotational system (called up at least once a month for two days during their time off, and in crisis situations – adequate to the scale of the threat). The most important tasks of WOT soldiers include: protecting the population and property from the effects of natural disasters and their removal, search and rescue operations, participation in crisis management tasks, cooperation with elements of the state defence system (in particular with provincial governors and local government), as well as shaping patriotic and civic attitudes.

In view of the increasing intensity of weather anomalies, protecting the population from the effects of natural disasters is one of the state's priority tasks, in which the WOT plays a leading role. The prerequisite for the high quality of the tasks performed by the formations is the constant improvement of cooperation and communication between the WOT and local government, the WOT and the police, the WOT and the Border Guard, the WOT and the State Fire Service, etc., as well as the gradual provision of modern equipment and intensive training.

In order to strengthen the scientific nature of the work, a research study was conducted to verify the main hypothesis, which was formulated as follows "*The Territorial Defence Forces are positively assessed by students in the area of*

1 Act of 11 March 2022 on the defence of the Fatherland (Journal of Laws 2022, item 655, as amended).

2 Ibid.

3 W. Kitler, J. Prońko, B. Wiśniewski, *Problems of crisis management in the state, study,* National Defence Academy Publishing House, Warsaw 2000, p. 3.

counteracting and responding to natural disasters, and their actions are perceived as effective, which justifies the systematic increase in the size of the formation".

The research used a diagnostic survey (quantitative method)[4], sample size: 310 national security students. The group was selected deliberately due to the knowledge possessed by students of the chosen field of study.

Preventing and responding to natural disasters – from definition to practical actions

A natural disaster is a serious, sudden event of a natural nature, causing significant damage, material losses, danger to life and significant disruption to the functioning of society[5].

A state of natural disaster, as one of the states of emergency specified in the Constitution of the Republic of Poland, may only be declared on the basis of an act of law (Article 228(2) of the Constitution of the Republic of Poland)[6]. The procedure for declaring and lifting a state of natural disaster, the rules of operation of public authorities and the scope of permissible restrictions on human and civil rights and freedoms are specified in the Act of 18 April 2002 on the state of natural disaster. This state may be declared both in the area affected by the disaster and in areas where its effects have occurred or may occur. It is declared by way of a regulation, on the initiative of the Council of Ministers or at the request of the competent provincial governor[7].

Types of natural disasters:

- Hydrometeorological: floods, droughts, hurricanes, tornadoes, lightning strikes;
- Geophysical: earthquakes, tsunamis, volcanic eruptions, landslides;
- Biological: disease epidemics, pest infestations;
- Climatic: extreme heat waves and cold spells[8].

Key organisational measures for prevention and response:

1. Forecasting – including meteorological, volcanological and biological forecasts.
2. Disaster response – alerting and warning the population, organising evacuation from endangered areas.
3. Rescue operations, including:
   - specialist reconnaissance;
   - assessment of losses and damage;
   - determining the extent of areas affected by destruction, fires and flooding;
   - identification of buildings and places of residence directly at risk;
   - assessment of the forces and resources necessary to locate threats and secure the population;

4 K. Żegnałek, *Research Methodology for Authors of Master's and Bachelor's Theses in Pedagogy,* WSP TWP Publishing House, Warsaw 2010, p. 88.

5 R. Grodzki, *Crisis Management Good Practices,* Difin SA Publishing House, Warsaw 2012, p. 171.

6 Constitution of the Republic of Poland of 2 April 1997.

7 Act of 18 April 2002 on the state of natural disaster (Journal of Laws 2002 No. 62 item 558, as amended).

8 Act of 18 April 2002 on natural disasters (Journal of Laws 2002 No. 62, item 558, as amended).

- assessment of the forces and resources needed to eliminate the effects;
- rescuing people;
- providing first aid;
- maintaining order and security;
- securing the property of victims;
- carrying out protective work;
- searching for missing persons.

4. Providing necessary assistance to victims in areas affected by disasters.
5. Reconstruction of destroyed infrastructure in cities, towns and regions.
6. Implementation of engineering and technical projects to strengthen resilience and reducing risk in the future[9].

The Armed Forces of the Republic of Poland are one of the most important pillars of national securityand are directly involved in every stage of the projects described[10]. The Territorial Defence Forces are of particular importance in the implementation of tasks related to combating natural disasters.

The developed model of calling up territorial service soldiers enables flexible and immediate deployment of military forces. Soldiers from brigades stationed in given provinces are sent to threatened or destroyed areas first. The delegation of soldiers to local tasks means that soldiers familiar with the topography, environmental conditions and specific characteristics of the community operate in the most sensitive areas, which translates into faster reconnaissance, more effective coordination and greater public acceptance of the activities.

Tasks of the territorial defence forces in the crisis management structure of the Ministry of National Defence

One definition presents crisis management as a system of activities regulating the functioning of an organisation in accordance with its objectives[11]. According to this approach, it is a complex process of designing and improving organisational structures, aimed at achieving high effectiveness and efficiency of operation.

Crisis response includes the actions of emergency services in response to events that threaten human life and health or the environment, aimed at limiting or eliminating the effects and providing assistance to those affected.

There are four phases of crisis management:

- prevention;
- preparation;
- response;
- recovery.

9 *Natural disasters,* https://www.jablonowopomorskie.pl/asp/pliki/obrona cywilna2019/ kleskizywiolowe.pdf, [accessed on 29 November 2025].

10 G. Piątkiewicz, *Challenges for the Armed Forces of the Republic of Poland based on the Act on the Defence of the Homeland and membership in the North Atlantic Alliance,* Res Politicae, vol. 16, (2024), p. 150.

11 W. Kitler, J. Prońko, B. Wiśniewski, *Problems…,* op. cit., p. 53.

These phases form the so-called security chain. Effective security building requires that it be part of a planned, well-thought-out and efficient process known as security management[12]. Even the best-organised activities will not bring the expected results without properly set priorities and hierarchies.

The Armed Forces of the Republic of Poland, with their considerable human and equipment potential, play a key role in the security management system. The Territorial Defence Forces occupy a special place in this area.

The Territorial Defence Forces are the fifth branch of the armed forces, alongside the Land Forces, Air Force, Navy and Special Forces. Their functioning is defined by internal acts of the Minister of National Defence and procedures established by the relevant commands.

On 25 April 2016, the Minister of National Defence approved the "Concept for the creation of the Territorial Defence Forces", which accelerated the development of the new formation[13]. The current commander of the Military Commando Unit, Colonel Wiesław Kukuła, was appointed commander of the WOT. On 21 December 2016, a new version of the Act on the Universal Duty of Defence of the Republic of Poland was announced, formally establishing the WOT as the fifth branch of the Armed Forces.

From 1 January 2017 to 13 August 2024, the WOT was directly subordinate to the Minister of National Defence. On 14 August 2024, it was subordinated to the General Staff of the Polish Army. This change strengthened the integration of the WOT with the entire command system and supported its role in the area of security management.

Organisational structure of the Territorial Defence Forces. The formation comprises: 18 brigades, two training centres, the Gryf Unconventional Warfare Unit, the SONDA Non-Commissioned Officers School and the Command Battalion. Among the eighteen brigades, there are two Border Defence Component brigades: the 19th Nadbużańska and the 20th Przemyska.

In 2024, one light infantry battalion in the 1st Podlasie and 4th Warmia-Masuria Territorial Defence Brigades was transformed into border defence battalions. Ultimately, from 2026, the 1st Podlasie and 2nd Lublin Territorial Defence Brigades will obtain the status of border defence brigades. In total, there will be four such brigades operating within the WOT structures[14].

12 E. W. Roguski, *Regional and Local Crisis Management in EU Standards,* Main School of Fire Service Publishing House, Education and Rescue Technology Foundation, Józefów 2006, p. 4.

13 M. Klisz, *Creation of Territorial Defence Forces as a response to new threats to national security,* Andrzej Frycz Modrzewski University Publishing House, Krakow 2017, p. 68.

14 G. Piątkiewicz, *The role of the Territorial Defence Forces in ensuring continuity of operations in the area of combating natural disasters,* [in:] N. Prusiński, The Polish Armed Forces in the protection and defence of facilities of particular importance to national security, Kalisz 2025, p. 48

The Border Defence Component created in this way will be responsible for the defence of border areas. Ultimately, 50,000 soldiers (approx. 45,000 rotational soldiers and 5,000 professional soldiers) will serve in the WOT[15].

The Territorial Defence Forces play a key role in:

- maintaining universal readiness to defend the Republic of Poland;
- protecting the population from the effects of natural disasters and in eliminating those effects;
- protecting property;
- conducting search and rescue operations and saving or protecting human life and health;
- participating in crisis management tasks;
- cooperating with elements of the state defence system, in particular with provincial governors and local government bodies;
- shaping patriotic and civic attitudes and values in society.

Pursuant to the Decision of the Minister of National Defence of 25 June 2018, the Territorial Defence Forces were incorporated into the Crisis Management System of the Ministry of National Defence (SZK RON)[16]. The aim of this integration is to ensure rapid and effective assistance to the population and support for local authorities. As part of the SZK WOT, a system for monitoring, analysing and assessing the likelihood of threats has been created.

The main element of the SZK WOT are the forces and resources at the disposal of the WOT Commander for the implementation of crisis management tasks. The Support Assessment Teams (SAT) and Reconstruction Support Teams (RST) also play an important role.

- SATs are responsible for reaching the scene of an incident as quickly as possible, reconnaissance of the area and preliminary assessment of the situation (scale of damage, needs, recommendations for the use of forces and resources).
- RST operate in the reconstruction phase, filling the gap left by the forces used in the immediate crisis response; they support reconstruction and clean-up work, coordinate support with local governments and services (e.g. logistics, engineering), contributing to a faster return of the community to normal functioning[17].

The Act of 23 April 2022 on the Defence of the Homeland entrusted the Territorial Defence Forces (WOT) with new tasks in the area of crisis management, including:

- transferring the non-military part of crisis management tasks in the Ministry of National Defence to the WOT;
- establishing the WOT Commander as the Head of the Ministry of National Defence Crisis Management Centre, responsible for coordinating activities;

15 *Structure and tasks,* https://www.gov.pl/web/obrona-narodowa/struktura-i-zadania, [accessed on 29 November 2025].

16 *WOT crisis management system,* https://www.wojsko-polskie.pl/dwot/wola-wot-w-zk, [accessed on 29 November 2025].

17 Crisis management information, https://media.terytorialsi.wp.mil.pl/informacje/kategoria/4999, [accessed on 29 November 2025].

– transferring the competences of the current heads of Provincial Military Staffs in the field of crisis management to the commanders of Territorial Defence Forces brigades, which means coordinating and implementing support provided to provincial governors[18].

As a result, Territorial Defence Force brigade commanders were obliged to cooperate on an ongoing basis with provincial governors and local government authorities. They are part of provincial crisis management centres, where, together with other entities, they conduct ongoing monitoring and analysis of the situation and participate in the development of action plans. In addition, the WOT Commander is required to participate in crisis staff meetings, is responsible for appointing civil-military teams and delegating soldiers to assess and diagnose needs in areas affected by threats.

Use of WOT soldiers in Operation Phoenix. From 23 September 2024 to 30 April 2025, Territorial Defence Force soldiers carried out tasks in flood-affected areas, participating in the largest military operation since 1989 – Operation Phoenix[19]. Over 13,000 soldiers were involved in the operation, including over 2,000 from the Territorial Defence Force[20].

The main tasks of the WOT soldiers included:

– mitigating the effects of flooding;
– accelerating the reconstruction of infrastructure;
– reducing the risk of localised flooding;
– improving the safety of the population;
– strengthening and repairing flood embankments.

WOT soldiers carried out operations in Gryfino, Zatonie, Raduszec Stary, Czerna, Wilków and Żelaźno, among other places. The work focused on cleaning up flooded areas (including public facilities) and, in cooperation with engineering troops, also on rebuilding flood defences, clearing roads and towns of debris and waste, and unblocking culverts under roads[21]. Below are the areas where WOT soldiers carried out their tasks as part of Operation Phoenix:

Lower Silesian Province

– **Counties:** Bolesławiec, Dzierżoniów, Jawor, Kamienna Góra, Karkonosze, Kłodzko, Legnica, Lwówek Śląski, Lubań, Świdnica, Wałbrzych, Ząbkowice Śląskie, Zgorzelec, Złotoryja.
– **Municipalities:** Oława urban municipality; Oława rural municipality (Oława County); Kąty Wrocławskie, Mietków, Sobótka (Wrocław County).
– **Cities with county rights:** Jelenia Góra, Legnica, Wałbrzych.

18 Act of 11 March 2022 on the defence of the Fatherland (Journal of Laws 2022, item 655, as amended).

19 *End of Operation FENIKS. The army remains in place,* https://media.terytorialsi.wp.mil.pl/informacje/850969/koniec-operacji-feniks-wojsko-zostaje-na-miejscu, [accessed on 2 October 2025].

20 The army is still fighting the effects of the disaster, https://media.terytorialsi.wp.mil.pl/informacje/841605/wojsko-wciaz-walczy-ze-skutkami-kataklizmu, [accessed on: 02.10.2025].

21 *Territorial Defence Forces,* https://www.gov.pl/web/obrona-narodowa/wojska-obrony-terytorialnej, [accessed on: 02.10.2025].

Opole Province
- **Counties:** Brzeg, Głubczyce, Kędzierzyn-Koźle, Krapkowice, Nysa, Opole, Prudnik.
- **Municipality:** Strzeleczki (Krapkowice County).

Silesian Province
- **Counties:** Bielsko, Cieszyn, Pszczyna, Racibórz.
- **City with county rights:** Bielsko-Biała.

Lubusz Province
- **Municipalities:** Szprotawa (urban-rural municipality), Żagań (rural municipality, Żagań County).
- **Cities:** Żagań, Małomice[22].

In Operation Phoenix, constant and close cooperation with government and local authorities, based on trust and efficient coordination of activities, was of key importance. The priority was to strengthen internal security and support the civilian population, especially in rebuilding the destroyed infrastructure. In carrying out these tasks, the Territorial Defence Forces clearly contributed to increasing the sense of social security[23].

Disaster response system in the European Union

The European Union (EU) programme for 2021 on disaster prevention and response is part of a broad initiative to strengthen the resilience of Member States and improve the effectiveness of crisis response[24]. a key tool is **the EU Civil Protection Mechanism**, whose functions include[25]:
- supporting cooperation between national civil protection authorities;
- raising public **awareness of risks** and preparedness for disasters;
- ensuring rapid, effective and coordinated assistance to countries affected by disasters.

The operational centre of the Mechanism is the Emergency Response Coordination Centre (ERCC), which operates 24 hours a day and coordinates the EU's response to emergencies.

Key elements of the programme[26]:
- the EU Civil Protection Mechanism;
- European Union Solidarity Fund (EUSF);
- priority for sustainable risk management;
- integration of climate change issues into risk management strategies;
- international cooperation.

22 *Areas affected by flooding*, https://www.gov.pl/web/arimr/tereny-dotkniete-powodzia, [accessed on: 03.10.2025].

23 G. Piątkiewicz, *The role*…, op. cit., p. 51.

24 Regulation (EU) of the European Parliament and of the Council of 20 May 2021 amending Decision No 1313/2013/EU on the Union Civil Protection Mechanism (2021/836).

25 Ibid.

26 Ibid.

In March 2022, the Council of the EU adopted conclusions on civil protection, emphasising, among other things:

– investment in research and innovation;
– the development of prevention and preparedness measures;
– strengthening civil protection capabilities;
– better preparation of citizens through wider access to information;
– encouraging citizens and volunteers to participate in civil protection initiatives.

The European disaster response system operates in three modes: monitoring, information exchange and full activation (Table 1), which are triggered depending on the scale and type of threat. It is worth noting that none of the modes is directly related to conducting operations in the affected area, which confirms the coordinating nature of this system.

Table 1. Modes of operation of the European disaster response system

Modes of operation of the European disaster response system			
Element/Service	Monitoring	Information exchange	Full activation
Exchange of existing emergency reports	✓	✓	✓
24-hour contact point	✓	✓	✓
Analytical reports		✓	✓
Platform for gathering and sharing information		✓	✓
Crisis meeting (ambassadors/ministers)			✓
Proposals for EU action			✓

Source: Own work: *New European system for combating natural disasters,* https://ec.europa.eu/commission/presscorner/detail/pl/ip_17_4731, [accessed on 2 October 2025].

The European Union does not have its own permanent forces and resources that could be deployed to the scene of an incident in an emergency. For this reason, it is necessary to develop clear procedures and rules of operation in the event of a crisis, so as to ensure maximum effectiveness of interventions.

In the coming years, the EU is likely to face increasingly frequent multidimensional crises, often occurring simultaneously in different regions. It will be crucial to increase the resilience of the community, as well as to ensure effective crisis communication and combat disinformation.

An important financial instrument is the European Union Solidarity Fund (EUSF), established in 2002, which provides support to regions affected by natural disasters. Member States can apply for funding in the event of floods, forest fires,

earthquakes, storms, droughts and public health threats (e.g. the COVID-19 pandemic). To date, the fund has been used in response to 118 natural disasters and 20 public health emergencies[27].

Protection of the population against natural disasters in the People's Republic of China

In 2008, China faced the so-called "winter of the millennium" – one of the largest non-military undertakings in the country's history. It is estimated that approximately 180 million people were stranded at train stations, airports, on roads and railways[28]. The armed forces were called in to combat the effects of this unprecedented disaster: military district commanders were given responsibility for supporting the civil authorities, and operations were coordinated by a specially established centre, which, among other things, set up 70 military medical points[29]. The motto guiding the operations was: "when one place is in trouble, help comes from every corner".

The following forces and resources were sent to areas affected by frost and heavy snowfall to support the civil administration:

- 519,000 soldiers;
- 1.6 million reservists;
- 34,000 vehicles;
- aircraft (transport planes).

Military equipment was also used **in unconventional ways**:

- shooting at icy power lines to remove ice cover;
- air drops of food, medicine, blankets and warm clothing to places cut off from roads.

The scale and pace of the operations yielded measurable results: approximately 17,000 kilometres of roads were cleared and made passable, approximately 4.3 million people were evacuated, and over 2 million tonnes of material aid were transported to residents of the affected areas. In addition, soldiers involved in the operation collected approximately 123 million yuan (approximately 17.5 million USD) for the victims and donated over 15 million items of warm clothing[30].

The example of China shows that even in the face of a crisis of enormous scale, it is possible to respond effectively by fully mobilising the key links in the response system. This approach, in the spirit of the motto "when one place is in trouble, help comes from every corner", can serve as a guide for the European Union in building a system that effectively counteracts crisis threats and strengthens citizens' sense of security.

27 How does the EU respond to crises and build resilience?, https://www.consilium.europa.eu/ pl/policies/eu-crisis-response-resilience, [accessed on 02.12.2024].

28 R.K. Bhonsle, *China: The Dragon's Winter Tsunami,* Boloji Media Inc., New York 2008.

29 Z. Śliwa, *The Chinese Armed Forces and Disaster Relief,* Przegląd Wojsk Lądowych, no. 6 (2009), p. 61.

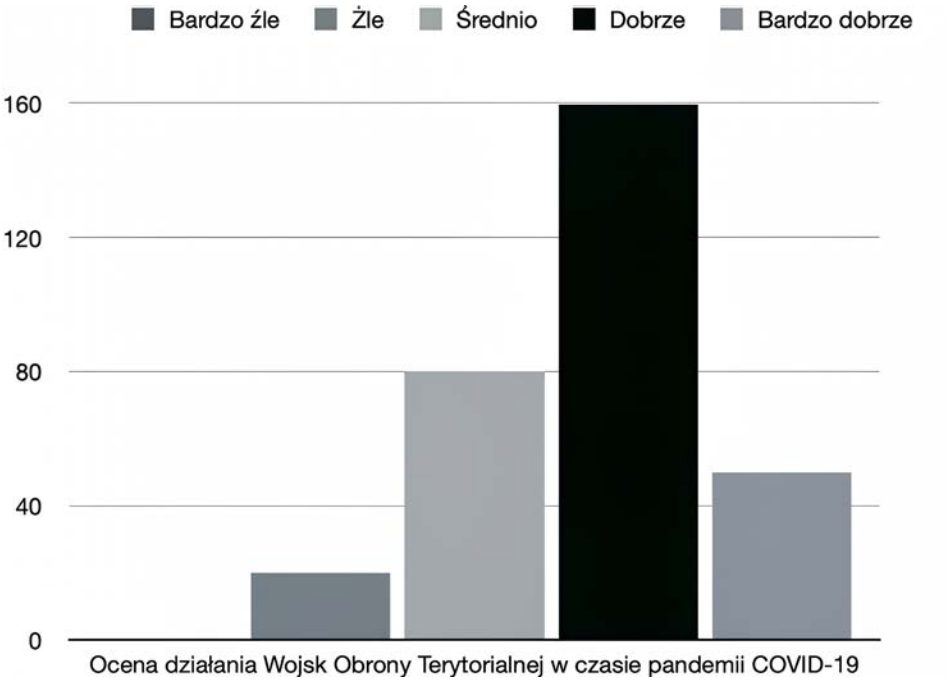
30 G. Piątkiewicz, *The* Role…, op. cit., p. 54.

Assessment of the performance of tasks by WOT soldiers

Building the potential of the Territorial Defence Forces based on soldiers performing territorial military service distinguishes this formation from other types of the Armed Forces of the Republic of Poland. Its specificity lies in the possibility of combining service with professional work or study. In accordance with the Homeland Defence Act (Article 303(1)), an employer is obliged to release an employee for the duration of the tasks performed by a WOT soldier and, moreover, may not terminate their employment contract.

Initially, this model of service was met with mixed opinions among professional soldiers and the public, especially with regard to the level of training and the quality of task performance. Therefore, a survey was conducted among students of national security at one of the Silesian universities to find out their opinions on the activities of the WOT in the area of combating natural disasters.

Figure 1. Assessment of the Territorial Defence Forces' activities during the COVID-19 pandemic



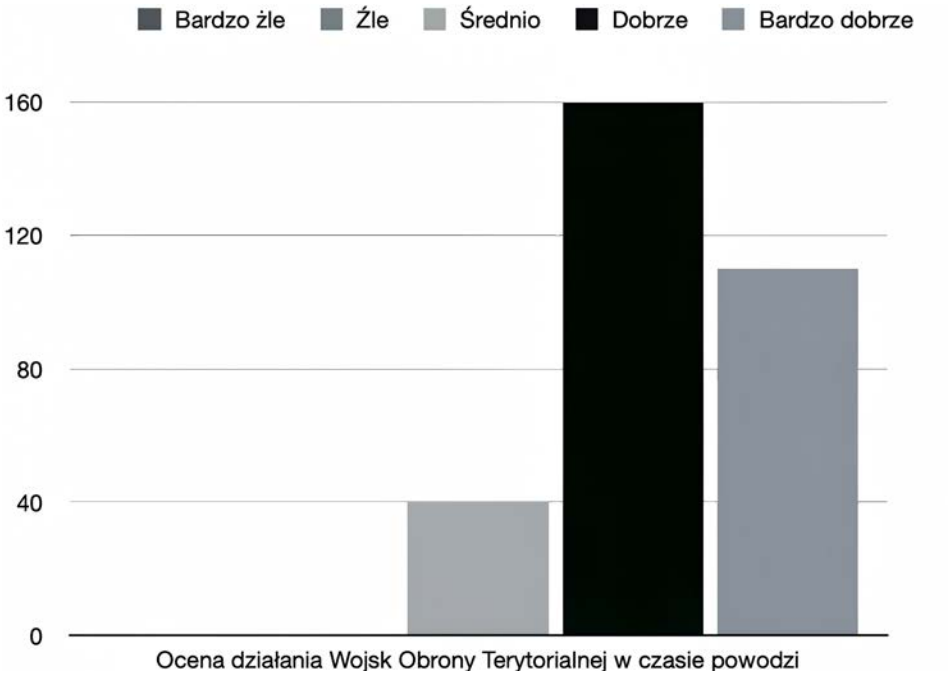
Source: Own work.

The activities of the Territorial Defence Force were rated negatively by 6% of respondents, and 26% of respondents rated them as "average" – which may be related to

the fact that this was the first such serious test for the formation, requiring above-average commitment.

However, the vast majority of students gave positive assessments: 52% rated the activities as good and 16% as very good. These results indicate that the tasks carried out mainly in support of the health service and the police were well received, despite the relatively limited experience of the Territorial Defence Forces soldiers.

Figure 2. Assessment of the Territorial Defence Forces' actions during the floods



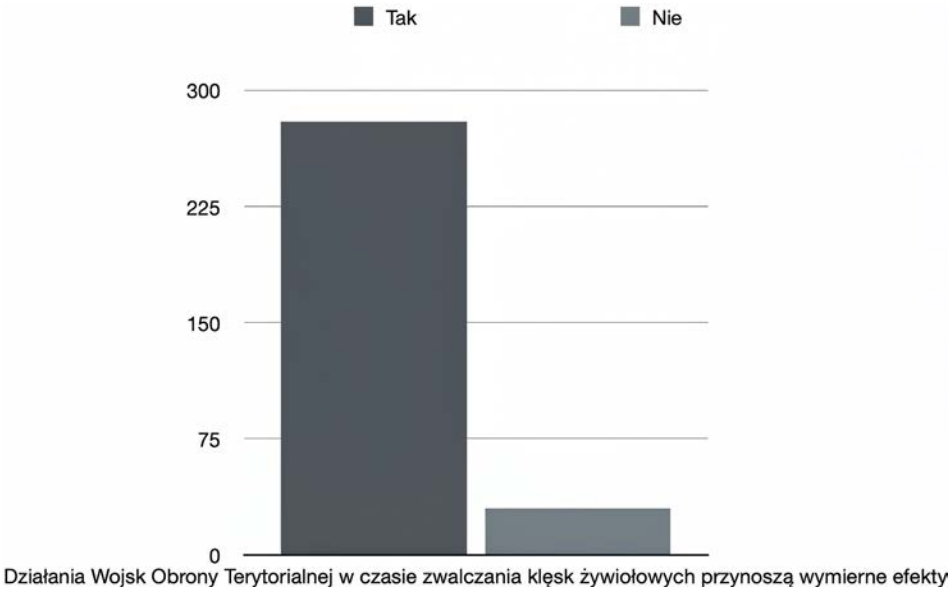
Source: Own study.

None of the respondents rated the actions of the Territorial Defence Force soldiers negatively. 13% of respondents rated them as average, while the vast majority of students gave them good (52%) and very good (35%) ratings.

Such a high level of acceptance may result from the trust built up by the formation during previous operations, especially during the COVID-19 pandemic, when protecting the Polish-Belarusian border and supporting the Border Guard on the Polish-Ukrainian border immediately after the outbreak of war in Ukraine.

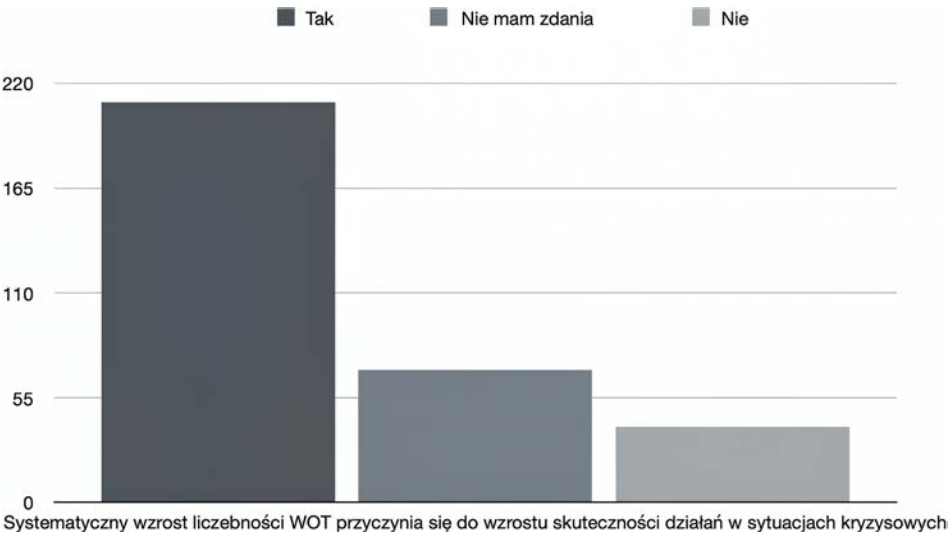
As many as 90% of respondents believe that the activities of the Territorial Defence Forces bring measurable results. This result confirms the high public support for the formation and the fact that soldiers, despite the rotational nature of their service, are regarded as professionals.

Figure 3. The activities of the Territorial Defence Forces in combating natural disasters bring measurable (visible) results



Source: Own study based on conducted research.

Figure 4. The systematic increase in the size of the Territorial Defence Forces contributes to the effectiveness of operations in crisis situations



Source: Own study based on the research conducted.

68% of respondents agree that the increase in the size of the Territorial Defence Forces increases the effectiveness of crisis response operations; 13% disagree with this opinion, and 19% have no opinion. These results suggest that respondents recognise the growing scale of military and non-military threats and are aware that the activities of the Territorial Defence Force contribute to increasing the level of national security.

Completion

Seven years after its formation, the Territorial Defence Forces have established themselves as an important component of the Armed Forces of the Republic of Poland in ensuring continuity of operations during natural disasters. Its effectiveness is due to its adequate organisational structure, intensive training system and operational experience gained, among others, during the COVID-19 pandemic, support for the protection of the Polish-Belarusian and Polish-Ukrainian borders, and in operations following the floods in 2024. The legal and organisational solutions applied allow for combining territorial military service with professional and educational activities, and open the path to professional service for the most distinguished soldiers.

Surveys conducted among students indicate that the WOT is generally viewed positively in the area of natural disaster prevention and response. Respondents attributed professionalism and effectiveness to soldiers, which, in their opinion, justifies a systematic increase in the size of the formation. The results confirm the thesis of growing public trust in the WOT and its real contribution to increasing the state's resilience to both military and non-military threats.

In the context of EU solutions, it should be emphasised that the EU's disaster response system, in place since 2021, is primarily of a coordinating and informational nature (modes: monitoring, information exchange, full activation). The lack of joint, permanent executive forces that can be immediately deployed to a crisis area limits the Union's ability to respond quickly to multi-focus events. From a public policy perspective, it therefore seems reasonable to: further strengthen mechanisms for joint planning and standardisation of procedures between Member States; consider building joint executive capabilities (military and civilian) dedicated to disaster response; integrating early warning, communication and logistics systems across the EU.

An analysis of China's experience with the so-called "winter of the millennium" (2008) shows that full mobilisation of state resources, clear assignment of responsibilities and centralised coordination of actions can significantly increase the effectiveness of crisis response. Although differences in political and institutional conditions do not allow for a simple transplantation of solutions , the very logic of action – rapid concentration of forces, interoperability of entities, priority for the

continuity of critical infrastructure and support for the population – can be treated as inspiration when designing European procedures.

Practical conclusions include: further strengthening the capabilities of the Territorial Defence Force in the areas of communications, reconnaissance, logistics and engineering support for reconstruction; developing interoperability with government and local government administration and emergency services; and systematically improving competence in crisis communication and countering disinformation.

In the area of further scientific research, it is recommended to continue measuring public opinion on representative research samples. These should be supplemented with an analysis of performance indicators, such as metrics of the time needed to restore functions in disaster-stricken areas, estimates of avoided costs, and indicators of the resilience of local communities.

In summary, the Territorial Defence Forces are an integral part of Poland's internal security architecture. Through the further development of specialist capabilities and closer cross-sectoral cooperation, this formation has the potential to become a model solution within an integrated disaster response system, both nationally and at European level.

Bibliography

Bhonsle R.K., *China: The Dragon's Winter Tsunami*, Boloji Media Inc. Publishing House, New York 2008.

Grodzki R., *Crisis Management Good Practices*, Difin SA Publishing House, Warsaw 2012.

https://ec.europa.eu/commission/presscorner/detail/pl/ip_17_4731.

https://media.terytorialsi.wp.mil.pl/informacje/841605/wojsko-wciaz-walczy-ze-skutkami-kataklizmu.

https://media.terytorialsi.wp.mil.pl/informacje/850969/koniec-operacji-feniks-wojsko-zostaje-na-miejscu.

https://media.terytorialsi.wp.mil.pl/informacje/kategoria/4999.

https://www.consilium.europa.eu/ pl/policies/eu-crisis-response-resilience.

https://www.gov.pl/web/arimr/tereny-dotkniete-powodzia.

https://www.gov.pl/web/obrona-narodowa/struktura-i-zadania.

https://www.gov.pl/web/obrona-narodowa/wojska-obrony-terytorialnej.

https://www.jablonowopomorskie.pl/asp/pliki/obrona cywilna2019/ kleskizywiolowe.pdf.

https://www.wojsko-polskie.pl/dwot/wola-wot-w-zk.

Kitler W., Prońko J., Wiśniewski B., *Problems of crisis management in the state, study,* National Defence Academy Publishing House, Warsaw 2000.

Klisz M., *Creation of Territorial Defence Forces as a response to new threats to state security*, Andrzej Frycz Modrzewski University Publishing House, Krakow 2017.

Constitution of the Republic of Poland of 2 April 1997.

Piątkiewicz G., *The role of the Territorial Defence Forces in ensuring continuity of operations in the area of combating natural disasters*, [in:] N. Prusiński, The Armed Forces of the Republic of Poland in the protection and defence of facilities of particular importance to state security, Kalisz 2025.

Piątkiewicz G., *Challenges for the Armed Forces of the Republic of Poland based on the Act on the Defence of the Homeland and membership in the North Atlantic Alliance*, Res Politicae, vol. 16, (2024).

Roguski E. W., *Regional and local crisis management in EU standards,* Main School of Fire Service Publishing House, Education and Rescue Technology Foundation, Józefów 2006.

Regulation (EU) of the European Parliament and of the Council of 20 May 2021 amending Decision No 1313/2013/EU on the Union Civil Protection Mechanism (2021/836).

Śliwa Z., *The Chinese Armed Forces and Disaster Relief*, Przegląd Wojsk Lądowych, No. 6 (2009).

Act of 11 March 2022 on the defence of the homeland.

Act of 18 April 2002 on the state of natural disaster.

Żegnałek K., *Research Methodology for Authors of Master's and Bachelor's Theses in Pedagogy*, WSP TWP Publishing House, Warsaw 2010.

About the Author

Major **Grzegorz Piątkiewicz**, PhD, Polish Army officer, assistant professor in the Department of Security Studies at Jan Długosz University in Częstochowa. Graduate of the Academy of Land Forces named after General Tadeusz Kościuszko in Wrocław, the Academy of Philosophy and Pedagogy in Kraków and the Higher School of Security in Poznań. He obtained his doctoral degree in social sciences at the University of the Commission of National Education in Kraków, at the Faculty of Pedagogy and Psychology. His doctoral dissertation was on socio-professional inclusion of International Security Assistance Force (ISAF) soldiers in Afghanistan. Master's degree in clinical psychology and re-socialisation pedagogy.

Expert in the Cybersecurity and Disinformation Research Laboratory. Department of Security Sciences, UJD, Częstochowa.

Since April 2001 continuously associated with the Military Police. Participant of foreign missions in Afghanistan, Kosovo and Sicily. Awarded numerous medals, including the "Star of Afghanistan and the Mediterranean Star" by the President of the Republic.

Rafał Magoń, PHd student
WSB University in Dąbrowa Górnicza
e-mail: r.magon@portal.ron.int
ORCID: 0009-0006-1873-950X

DOI: 10.26410/SF_2/25/3

DEFENSE AND PROTECTION OF THE BORDER IN RELATION TO STATE SYSTEMS IN TIMES OF WAR AND PEACE

Abstract

The authors aim to characterise the challenges related to securing the state border during both peace and war times. First, they concentrate on the individual formations of uniformed services at work. These formations are responsible for defending the civilian population and the state institutions in the area of Poland's eastern border. The authors outline the legal framework that defines and constrains the functioning of entities responsible for border protection and defence in both countries. The cooperation between various uniformed formations in response to the challenges on Poland's eastern border is described and analysed. Additionally, through an examination of the current legal status and the practical responses to these challenges, they suggest solutions for enhancing the protection and defence of Poland in peace and war.

Keywords

border, defence, security, uniformed formations

Introduction

Ensuring public safety and maintaining stability at the national border are among the most important tasks carried out by the armed forces stationed at the country's borders. The safety of civilians living in border areas depends on how well the armed forces organise their work. It should be noted that the measures taken must be supported by good technical assistance to aid the armed forces' efforts. The current situation on the eastern border, with the proximity of the Russian-Ukrainian conflict, the issue of illegal migration, and the terrain of the border, presents very serious logistical and defence challenges for law enforcement.

However, to consider the role of representatives from individual law enforcement agencies, it is first necessary to define the concept of security and the protection of national borders. According to the basic definition, 'security' is a situation in which a person, as an individual or an entire social group, as well as an organisation or a state, does not feel any threat to their existence and can clearly pursue their goals and interests. Ensuring security involves both the absence of an objectively perceived threat and the subjective perception of a dangerous situation[1]. The state of security directly influences people living in a given area and, from a cultural perspective, helps shape the state. Legally, the concept of the state as a functioning structure is complemented by cultural and ethnic elements related to the characteristics of a nation with a rich tradition. The population residing in a given area, communicating in the same language and striving to achieve shared social goals, begins to form the foundation of a community called society. The functioning of society in a specific area is determined by the use of a common language, shared culture, as well as by common experiences–both good and bad–, the possession of the same or similar national consciousness (also known as national identity), and a unified, organised legal framework. This includes a structured social hierarchy with representatives performing specific functions aimed at maintaining the proper operation of social structures[2]. Furthermore, it should be emphasised that a nation is a single political entity or, in other words, a community consisting of different peoples, nationalities, a political community of all inhabitants living in a given territory, operating under a uniform law and forming a civil society. Thus, a nation is not only a specific component of the state institution but also an entity that contributes to its security[3]. Generally, the state as a unified social entity is not the sole defining factor for the existence of the state itself. This relates to the fundamental determinant of the state's functioning and existence–its inhabitants, i.e., the population. It is the society permanently residing within and represented by its authorities that creates a unified

1 Sójka W., Gąsiorek K., *Ochrona, obrona i bezpieczeństwo granicy państwowej w warunkach zewnętrznego zagrożenia państwa i w czasie wojny*, Warszawa 2021.

2 Leszczyńska K., *Poza granicami. Płeć społeczno-kulturowa w katolickich organizacjach migracyjnych*, Wydawnictwo Nomos, Kraków 2020.

3 Lubiewski P., *Granice Rzeczypospolitej Polskiej jako wyzwanie dla bezpieczeństwa państwa*, Przegląd Policyjny (nr specjalny), Warszawa 2019.

state institution under the rule of law. Additionally, the state can be recognised as a fully functioning entity when diplomatic, consular, political, economic, commercial, and cultural relations are established with neighbouring countries. However, this definition is not entirely precise, as neighbourly contacts and relations can also be established between states that do not share a border. In practice, however, the role of neighbouring entities is most often taken up by directly bordering countries, which create specific ties in the fields of economy, politics, and cooperation[4]. From an organisational and institutional perspective, it is essential to mention the basis–or even the obligation–to ensure security within a given state for its citizens. For this purpose, organised structures of the state, local government, public administration, services, inspectorates, and guards, as well as armed forces organised hierarchically into an integrated national security system, are established. Since the state operates in many different areas, these bodies and institutions must be aware of the multitude of objectives arising from the interests and policies of the state. Therefore, when formulating the directions of state action, authorities aim to coordinate both the efforts of various services and the available resources, minimising losses[5].

There are multiple ways to ensure the secure functioning of the state. These include methods of maintaining civil security in terms of the stable operation of government bodies and organisations during peacetime, as well as the proper functioning of the executive and legislative branches. The main entities of the state's organised defence system are: the armed forces, civil public administration, diplomatic units, businesses, special services units, and all other non-governmental organisations. These entities are responsible for maintaining security and the proper operation of state organisations during periods of stability and peace[6]. Security also refers to a state or system of statehood designed to address challenges, reduce risks, and counteract external and internal threats of a civil (non-military) nature. This group of activities encompasses specific operational (interventional) elements developed to protect the state as a political (sovereign), territorial, legal, and coercive institution, and above all, as a social institution. Regarding security, it is essential to consider the full protection of the state and the constitutional order–not only safeguarding its structures but also each citizen as a social entity, along with their physical and intangible assets, and their surroundings, such as infrastructure and the natural environment, against all threats that could significantly hinder the functioning of both the state and individuals[7]. The potential protective bodies of the state include: the judiciary, special services, guards and inspections specialising in the protection

4 Kuśmirek, K. *Information activities during the migration crisis on the Polish-Belarusian border as a threat to society's resilience*. Bezpieczeństwo. Teoria i Praktyka, 48(3), (2022) 311–321.

5 Blicharz, J. Znaczenie ekonomii społecznej jako narzędzie rozwoju społeczeństwa obywatelskiego w kontekście dostarczania usług publicznych. W: L. Zacharko (red.), *Nauka administracji. Paradygmaty współczesnego zarządzania w administracji publicznej* (2016). (s. 51–64). Racibórz: Wydawnictwo PWSZ w Raciborzu.

6 Kitler, W. System ochrony państwa i jego porządku konstytucyjnego. *Wiedza Obronna*, Tom 268, Nr 3. (2019).

7 Zamiar, Z., & Zamiar, P. Pozamilitarne ogniwa w systemie bezpieczeństwa militarnego państwa. *Zeszyty Naukowe Wyższej Szkoły Oficerskiej Wojsk Lądowych im. gen. T. Kościuszki, (4/162)*, (2011). 91–98.

of security and public order, rescue and civil protection services, elements of crisis management, the Border Guard, the Customs and Tax Service (National Revenue Administration), private sector entities (personal and property security companies), and non-governmental organisations. These units operate during peacetime and are capable of functioning within the Polish state without conflict.

However, in certain circumstances, changes may occur, and in fact, security measures may be mobilised during conflicts in neighbouring countries, dangerous situations at the national border, as well as during times of war in neighbouring territories. Other executive subsystems established to support national security are systems designed to protect critical infrastructure. These include facilities and services essential for the functioning of the state and the security of its citizens. This covers areas such as energy, communications, transport, healthcare, water and food supply, strategic reserves, national border protection, flood defence, personal data protection, and classified information security. Within the framework of state action, support for national (state) security is enabled by the state's potential in the following subsystems: social, economic, energy, and transport[8]. In the authors' view, it is crucial to highlight individual specialised executive subsystems, emphasising their vital role in achieving the desired state of national security. Nevertheless, the core message of this article remains to underscore the role of individual armed services in ensuring security at various stages of the nation's operation, with a particular focus on the functioning of armed services in border regions.

Armed forces in border protection and security

The following armed forces are responsible for the proper functioning of state institutions, i.e., ensuring security during both war and peace, especially for civilians living and operating in border areas: the Border Guard, Armed Forces, and Military Police. These units may be supplemented by the Police and the Forest Guard. Additional reinforcement and deployment of armed forces beyond those permanently assigned to border protection can occur in response to a threat to border security, such as during armed conflicts involving military operations beyond the eastern border. After World War II, the army was the main military body responsible for safeguarding the security and operation of the Polish border. In September 1945, a border defence force was established–the Border Protection Forces (WOP). During the late 1980s and early 1990s, significant political and social changes took place in Central and Eastern Europe, including Poland. The Border Guard Act of 12 October 1990 led to the creation of the Border Guard (SG), which took over the duties of border protection and traffic control from the Border Protection Forces[9]. Issues such

8 Gąska, M., & Trubalska, J. (Red.). *Bezpieczeństwo narodowe i międzynarodowe Rzeczypospolitej Polskiej: wybrane problemy*. Lublin: Innovatio Press, (2015).WSEI.

9 Barszczewski W., Ciekanowski Z., Witkowicz S., *Specyfika działań Nadbużańskiego Oddziału Straży Granicznej dla zapewnienia bezpieczeństwa wschodniej granicy Unii Europejskiej*, Warszawa 2025.

as illegal immigration and threats along Poland's eastern border compelled armed forces to boost their combat readiness. As a result, the Polish Armed Forces, Police, and Forest Guard have all been involved in border security efforts[10].

Border Guard

Since Poland's eastern border also serves as the border of the European Union, basic defence activities in this area are closely linked to international security. It should be emphasised that the most important formation, and the first in its operations, is the Border Guard and its significant contribution to defending the European Union's border. Naturally, Poland's accession to the European Union required all authorities and services in Poland to adapt their activities to meet EU standards. However, the activities of the Border Guard are the most vital and foundational. The country's security is ensured by a common foreign policy established by the member states of the European Community. At the time of Poland joining the European Union, the structure and operations of the Polish Border Guard had to be adjusted accordingly. As a result, this organisation was transformed from a typical military unit into a service with police-like functions and powers. In 2006, the uniformed force was fully professionalised.

This effect was achieved by transforming the candidate service system, which was part of basic military service, into professional employment. At the start of 2001, Article 4 of the Border Guard Act, stating that the Border Guard would, by law, become part of the Armed Forces of the Republic of Poland in the event of mobilisation or armed conflict–forces entirely subordinate to the Ministry of National Defence–was completely repealed. Based on this change, the supervisory authority for the Border Guard, during times of national security threats and wartime, was also shifted to the Ministry of the Interior. Currently, the Border Guard's task is to carry out statutory and defence activities as specified within the ministry by the Minister of the Interior[11].

However, this was not the end of the structural and operational changes within the Border Guard. In 2002, further amendments were made to the Border Guard Act, which stipulated that, in the event of mobilisation and during wartime, the formation would undergo militarisation. The Act also included a clause stating that officers remaining in service during mobilisation or war would automatically become officers serving during the conflict, continuing in service until their discharge. Presently, the Border Guard collaborates directly with the army according to agreements between the Commander-in-Chief of the Border Guard, the Commander-in-Chief of

10 Szczurek, T. Ministry of National Defense in the Crisis Management System. *Roczniki Nauk Społecznych*, 15(51)(2), (2023). 7–18.

11 Celiński W., *Rola Straży Granicznej w systemie bezpieczeństwa narodowego*. Siedlce 2018.

the Armed Forces, and the Commander-in-Chief of the Military Police[12]. The Act on the Functioning and Tasks of the Border Guard outlines the full range of duties assigned to this armed entity, primarily comprising the protection of Poland's land and sea borders and the oversight of border traffic. The goal is to ensure national security. Based on this, Border Guard officers involved in safeguarding the Polish state border have the right to:

- Carry out direct and indirect border controls;
- Conduct personal checks on individuals at the national border, as well as inspect luggage contents, including checking cargo at ports and stations and in air, road, rail, and water transport. This aims to completely eliminate the possibility of committing crimes or offences, especially those directed against the sanctity of the state border or security in international transport;
- Conduct security checks at designated and other border crossings, as well as in all forms of air, road, rail, and water transport. This aims to prevent the possibility of crimes or offences being committed, particularly those targeting the inviolability of the state border or security in international transport;
- Conduct security supervision directly on board aircraft and have the authority to use all necessary measures, including direct coercive measures and service weapons, to remove persons who pose an immediate threat to flight safety, as well as to the health or life of passengers or crew members;
- Issue visas and other permits permitting citizens to cross the state border according to separate legal provisions;
- Verify the identity of persons crossing the national border or establishing their identity by other means, as well as detaining persons in the manner and in the cases specified in the provisions of the Code of Criminal Procedure and other separate legal regulations, and bring them to the competent Border Guard authority, court or prosecutor's office;
- Search persons, items, premises, and means of transport as specified in the provisions of the Code of Criminal Procedure, other laws, and legal regulations;
- Detain and return dangerous radioactive, nuclear (fissile), chemical, and biological materials, along with waste derived from them, from the national border to the sender[13].

To ensure the effective operation of the Border Guard, which is responsible for protecting Poland's border, a fundamental element supporting human activity was established. Consequently, a border road strip and a border zone were created, with specific areas (zones) clearly defined. The first and most immediate zone is the border strip. This zone extends 15 metres inland from the state border line, whether on land or from the shore of border waters or the sea coast. According to regulations, movement within the border strip is generally unrestricted, but to prevent violations,

12 Błażejczak, K. Miejsce Straży Granicznej w systemie bezpieczeństwa państwa a typologia grup dyspozycyjnych. *Społeczeństwo i Polityka*, 3(68), (2021). 95–116.

13 Celiński W., *Rola Straży Granicznej w systemie bezpieczeństwa narodowego*. Siedlce 2018.

it must be precisely marked and described. Clearly visible signs displaying 'National border – crossing prohibited' are placed in conspicuous locations. In certain urgent cases, when immediate border protection is required, the provincial governor of the area may temporarily impose a complete ban on unauthorised persons entering specific sections of the border road. This is enacted through a special request, usually supported by an opinion from the relevant state border protection authority. Additional, equally clear markings are also prepared, using signs bearing the inscription: 'Border road strip – no entry'. It is important to note that this prohibition does not apply to landowners or users within the border zone, nor to those on marked tourist routes, the seashore or bathing areas. The second key component in safeguarding Poland's borders and maintaining security is the border zone. This area encompasses the municipalities directly adjoining the national border and, in the maritime section, the seacoast. The zone extends another 15 km inland. If the border zone is less than 15 km wide, it also includes areas within municipalities that indirectly neighbour those bordering the border or coast. The responsibility for determining the boundary of the border zone and marking it with signs inscribed 'Border zone' lies with the Chief Commander of the Border Guard[14].

In the face of current threats caused by illegal immigration, it is the Border Guard officers who are responsible for countering illegal migration. All actions in this regard are directly based on Article 470 of the Act on Foreigners. These tasks involve monitoring strict compliance with regulations related to the movement of people in the border zone, such as the entry and residence of foreigners on Polish territory. Border Guard officers are tasked with identifying and analysing all migration threats, as well as combating them, particularly those that directly or indirectly lead to crimes related to illegal migration. The inclusion of the prevention and combatting of illegal migration in the list of strategic, legislative tasks of the Border Guard stems from the implementation of the Assumptions of the long-term concept for the functioning of the Border Guard developed for the years 2009-2015, under which the Border Guard is to become the leading migration service[15].

Armed Forces of the Republic of Poland

Between 2022 and 2025, the Polish-Belarusian border became a hotspot for intense hybrid activities, posing a serious challenge to Poland's national security and the European Union. This issue is linked to Belarus' aggressive policies and the so-called 'illegal immigration'. The phenomenon intensified notably after Belarus' highly controversial presidential elections, which triggered mass protests and repression of opposition activists. Alexander Lukashenko's dictatorial rule, combined with the country's international 'isolation', has resulted in measures such as using illegal

14 Konieczny M., *Status, rola i zadania Straży Granicznej w Polsce*, Kraków 2021.

15 Elak L., Oskierko M., Żurawski S., *Ochrona granicy polsko-białoruskiej w obliczu wojny hybrydowej*, Warszawa 2024.

migration as a tool to pressure neighbouring countries, especially Poland, Lithuania, and Latvia. The main strategy involved systematically bringing migrants from the Middle East and Africa to Belarus and then deploying them en masse to the border with Poland.

The primary aim is to destabilise Poland internally and exert political 'blackmail' by pressuring EU authorities. Another motive behind Lukashenko's actions is to distract from Belarus' internal issues. In response, Poland has implemented various measures to bolster border protection, including constructing physical barriers and increasing security personnel presence. As previously mentioned, the Border Guard remains the principal armed force responsible for eastern border security. However, in light of the illegal immigration threat and attempts to disrupt normal order, the Polish Armed Forces were deployed to support the Border Guard. Polish law provides several regulations permitting military involvement in border protection activities during such threats. According to Article 26(1) of the Constitution of the Republic of Poland of 2 April 1997, the army's primary duties are to defend the state's independence, territorial integrity, and ensure border security. Nonetheless, the Constitution does not specify how these tasks should be executed. During heightened demand, Border Guard officers can receive direct assistance from soldiers.

The legal basis for this is found in Article 27 of the Act of 4 September 2008 on the protection of shipping and seaports[16], and Articles 11b, 11c, and 11d of the Act of 12 October 1990 on the Border Guard[17]. Additionally, the Polish Armed Forces[18] may operate along the Belarus border under Article 11 of the Act of 21 June 2002 regarding states of emergency, to counteract destabilisation. Given the serious threat, fully legal procedures are crucial. After examining relevant legal frameworks, it was concluded that the Border Guard Act forms the foundation for military participation and presence at the border. This legislation permits the deployment of soldiers only in three specific situations, related to Articles 11b, 11c, and 11d. The third, related solely to the Military Police, is excluded since operations at the eastern border involve other branches of the Armed Forces[19]. When soldiers are assigned for defensive operations, the Commander-in-Chief of the Border Guard coordinates their activities, especially when multiple units operate in the same area, as specified in Article 11b(8)(227). Based on the above, these regulations serve as the legal basis for all military actions in the border region during actual threats linked to illegal migration. The involvement of Polish Armed Forces soldiers is thus justified to secure the border and uphold national sovereignty. It should also be emphasised that soldiers are only deployed when Border Guard capacity proves insufficient or when

16 Act of 4 September 2008 on the Protection of Shipping and Seaports, consolidated text: *Journal of Laws* 2024, item 597, Art. 27.

17 Act of 12 October 1990 on the Border Guard, consolidated text: *Journal of Laws* 2025, item 914, Arts. 11b–11d.

18 Regulation of the Council of Ministers of 31 August 2023 on cooperation between the Border Guard and units and subunits of the Polish Armed Forces, *Journal of Laws* 2023, item 1767.

19 Kośka M., *Ochrona lądowej granicy Rzeczypospolitej Polskiej z Republiką Białorusi w związku z kryzysem migracyjnym w okresie od lipca 2021 roku do czerwca 2024 roku*, Piotrków Trybunalski 2024

the threat level is elevated. Support operations by soldiers began in July 2021 with the formation of the GRANICA30 Task Force, comprising operational troops and Territorial Defence Forces personnel for auxiliary duties[20]. These soldiers conducted information campaigns for residents in emergency zones and assisted in building a temporary border barrier, which started near Szudziałowo in late August 2021. About 1,000 soldiers were initially involved, with numbers increasing by 2.5 times in September and reaching 15,000 by year's end[21]. The core activities include stationing at observation posts and patrolling on foot, both independently and alongside Border Guard officers. They also use drones for aerial patrols during day and night, and operate lighting masts at critical border points. Support from the Territorial Defence Force in Operation GRYF reports to border guards. As of August 2023, up to 4,000 soldiers were set to be involved, as decided by the Minister of National Defence[22]. On 12 August 2023, a separate task force was established during Operation RENGAW, comprising units including the 16th and 18th Mechanised Divisions, 17th Mechanised Brigade, the 6th Airborne Brigade, the 25th Air Cavalry Brigade, UAV bases, and specialised units like the Military Police and Special Forces. These units are equipped with various weaponry and engineering tools, including carbines, armoured vehicles, tanks, missile systems, helicopters, and surveillance equipment. They will also construct engineering barriers, bunkers, and firing positions across the border, under an agreement among Poland, Latvia, Lithuania, and Estonia[23].

Police

Ensuring security along the Polish-Belarusian border is not only the result of actions by individual armed forces, including the Border Guard and the Polish Armed Forces, but also relies on cooperation with other units, such as the police. Long before the migration crisis on the eastern border, in 2004, the Border Guard and the police signed a cooperation agreement. The document clearly specified and defined the framework for this cooperation. The police, together with representatives of the Border Guard, undertake to:

- cooperate in combating and preventing crime, in particular in identifying terrorist threats, as well as actively participating in the protection of the nation's border;
- police officers will carry out preventive protection and strictly ensure public safety and order on the border;

20 Kukuła, W., *Siły Zbrojne w systemie reagowania na kryzys migracyjny na granicy z Republiką Białorusi – wyzwania i doświadczenia* [Wystąpienie konferencyjne]. Konferencja „Bezpieczeństwo granicy państwowej w kontekście kryzysu migracyjnego", Warszawa 2023, wrzesień 15.

21 Waniek, P., & Brążkiewicz, D. Kryzys migracyjny na granicy polsko-białoruskiej. W: D. Brążkiewicz, J. Nowicka, Z. Ciekanowski, & L. Elak (red.), *Współczesne wyzwania dla bezpieczeństwa państwa*, 2023, (ss. 47–60). Wydawnictwo im. prof. Leszka J. Krzyżanowskiego.

22 Nowak T., *Wzmacnianie bezpieczeństwa militarnego Polski na ścianie wschodniej*, Piotrków Trybunalski 2023.

23 Ochyra, P., Brążkiewicz, D., Żurawski, S., & Ciekanowski, Z. *Siły Zbrojne RP jako element zarządzania kryzysowego w Polsce* [The Polish Armed Forces as an element of crisis management in Poland]. Studia Administracji i Bezpieczeństwa, 16(16), 2024,. 291–307.

– the basis for cooperation between the police and other representatives of the defence forces will be the continuous improvement of the methodology of performing tasks and official duties, as well as active logistical support.

The process of cooperation between the Border Guard and the police will mainly involve information exchange, joint actions–especially when they concern persons or objects of mutual interest–and the provision of specialist support and mutual logistical services[24]. On behalf of the police, the following are authorised to collaborate with Border Guard units: the Chief Commander of the Police, the Provincial Commander of the Police, the District (Municipal, Regional) Commander of the Police, and the Chief of the Police. As part of the signed agreement, a catalogue of events has been established, which the Border Guard is obliged to report to the police, and vice versa. Furthermore, tasks and parameters have been developed to guide the flow of information between the two cooperating units. For example:

If any incident occurs at the border suggesting the possibility of preparing or attempting to commit a prohibited act, which is nominally the responsibility of the police to prosecute, all related information must be immediately forwarded to the duty officer at the relevant local unit. As a result of this information flow, the Border Guard is obliged to notify the police of the incident. a similar procedure applies when there is suspicion of an illegal gathering or assembly in the cross-border area that disrupts public peace and order. The same applies to the detection of any event in the border zone that poses a collective threat to public safety, transport safety, or environmental safety. In such cases, information is also passed from the Border Guard to the police. However, in incidents involving individuals and criminal groups clearly engaged in smuggling immigrants, smuggling goods, or falsifying documents granting the right to cross the national border, the information is immediately forwarded upon receipt. This information should be relayed to the duty officer at the relevant territorial unit of the Border Guard. Consequently, it is the police that notify the Border Guard[25]. Police officers perform all duties assigned to them regarding border protection and the preventive safeguarding of public safety and order from the moment Poland joined the Schengen area. Therefore, close cooperation and coordination between the police and other law enforcement agencies present at the border are essential for success. The police and Border Guard collaborate through joint patrols and share various tasks related to border protection in an appropriate manner. An example of such cooperation is roadside checks in the border area, particularly on access routes to the border. Police and Border Guard patrols undertake tasks specified in the agreement on cooperation between the police and the Border Guard. The primary focus of these tasks is to ensure security and uphold public order near border crossings. During their joint operations, police and Border Guard officers work together to apprehend individuals illegally crossing the border. Officers of both

24 Jakubczak, R., *Use of genocide by the Russian Federation in the conduct of hybrid activities and warfare in Ukraine*. Studia Prawnicze KUL, 4, 81–99, 2024.

25 Płaczek, A., Policja i jej rola w ochronie granicy państwowej. *Przegląd Policyjny*, 29(nr specjalny), 2019, 87–97.

services also carry out measures to counter illegal migration. It is worth emphasising that, amid the migration crisis on the eastern border, the primary objective of cooperation between the Border Guard and police is to combat organised criminal groups, including international ones, involved in smuggling, drug trafficking, and human trafficking. To achieve this, coordination teams comprising officers from both services are established. According to recent data, over 2,000 officers serve in the Podlasie Border Guard Unit. These forces are supported by both police personnel and the army. The combined efforts of these three armed forces have led to a marked decline in illegal border crossings in the Podlasie Province. According to information from the Ministry of the Interior and Administration, 4,276 attempts to illegally cross the border were recorded between 13 June and 20 August 2024. In comparison, before the establishment of the buffer zone, over 13,675 such attempts were detected in a similar period from 5 April to 12 June 2024. Since 13 June 2024, over 1,800 police officers have been engaged in guarding Poland's eastern border with the Republic of Belarus. The officers conduct numerous training courses for Border Guard and military personnel on the operation of specialised units. Currently, approximately 5,500 soldiers from various formations of the Polish Armed Forces are stationed along the border with Belarus. Throughout the entire 'Safe Podlasie' operation, which commenced on 1 August 2024, around 17,000 soldiers will participate on a rotational basis. The core of the operation comprises units of the 18th Mechanised Division, supported by subunits of the General Command of the Armed Forces, the Military Police, the Territorial Defence Forces, and the Armed Forces Support Inspectorate. The army remains prepared to provide any necessary assistance to the Border Guard and Police at any time[26].

Forest Guard

It is also worth mentioning other groups and formations that can help temporarily secure the eastern border, especially amid the migration crisis. One such formation is the Forest Guard. The presence of its officers on patrols and close cooperation with the already discussed units of the Border Guard, the Polish Armed Forces, and the Police aims to ensure even greater effectiveness in maintaining security in this challenging region of our country. As part of close cooperation in the border area, it should be remembered that not only people (permanent residents, migrants) appear there, but also animals and plants. Therefore, all matters related to the protection of flora and fauna in the municipalities and counties along the borders must be properly managed. Since the Polish-Belarusian border area is mainly forested, these areas remain under the jurisdiction of the Forest Guard, the National Park Guard, and the State Hunting Guard. The tasks of the first of these formations include, in particular: managing forests run by the State Forests, forest

26 Kośka M., *Ochrona lądowej granicy Rzeczypospolitej Polskiej z Republiką Białorusi w związku z kryzysem migracyjnym w okresie od lipca 2021 roku do czerwca 2024 roku*, Piotrków Trybunalski 2024

management and protection, combating crimes and offences related to forest damage and nature conservation, and performing other tasks related to property protection. Although during times of peace and stability at the border, Forest Guard and National Park Guard officers mainly perform educational activities for the public and are involved in protecting plants and animals, in times of heightened threat, such as the migration crisis, these services are tasked with actively supporting other uniformed services involved in border defence and regional security[27]. In 2021, the State Forests announced that Forest Guard officers would be deployed to the Belarus border to support the Border Guard, Police, and Polish Army in defence operations. The designated Forest Guard officers were sent to border units. According to the State Forests' statement, Forest Service officers possess the relevant experience, vehicles, and equipment necessary to fully support other law enforcement agencies during crises. The advantage of local Forest Guard officers is their excellent knowledge of the terrain, especially inaccessible forest areas, which has helped increase the effectiveness of security services in defending Poland's eastern border[28].

To ensure the continuity and stability of state border protection, especially during a migration crisis, it is essential to identify the main directions for enhancing cooperation among the various law enforcement agencies operating at the border to secure and defend it. These measures should include the comprehensive integration of the national security management system, as well as increasing the resilience of the state, including the protection of the population and civilians, and developing a universal defence system. It is very important to strengthen collaboration between the Ministry of National Defence and various pro-defence organisations to support the training of human reserves and to enhance the capabilities of the Border Guard. Additionally, it is necessary to focus on upgrading and expanding existing infrastructure, including barrier systems, and improving the ability to respond to threats such as cyberattacks and hybrid activities emerging from the eastern aggressor. Providing Polish Army soldiers with adequate logistical equipment and training support is vital for more effective border patrols and threat countermeasures, as well as ensuring smooth cooperation with existing pro-defence organisations in areas such as reserve training, logistical support, and defence activities. This might involve regular military and defence exercises that include not only pro-defence organisations but also the civilian population to improve border defence procedures and skills. Furthermore, conducting numerous information campaigns to raise public awareness about the threats and the importance of defending the eastern border is crucial.

27 Kobus, I., *Straż Leśna w systemie bezpieczeństwa wewnętrznego* [Forest Guard in the internal security system]. Bezpieczeństwo. Teoria i Praktyka, 8(2), 2014,. 51–61

28 Stec, R., *Komentarz do art. 53* [w:] B. Rakoczy, A. Woźniak, & R. Stec (red.), Prawo łowieckie. Komentarz. LEX (SIP LEX), 2014.

Conclusions

Ensuring public safety and maintaining stability at the national border is among the most vital tasks undertaken by the armed forces stationed there. Law enforcement agencies established specifically for this purpose are involved in maintaining order and security on Poland's eastern border. This remains true both in times of peace and during threats of war or other crises in these areas. The primary unit tasked with defending the border is the Border Guard. Its activities are a priority in preserving peace and supporting the proper functioning of the population in this region, thereby ensuring the stability of the Polish state. However, in periods of unrest or an intensified migration crisis, the Border Guard may be supported by other armed forces. As demonstrated in this study, officers from the Polish Armed Forces, the Police, as well as local representatives of the Forest Service or the National Park Guard, may be delegated to assist in these efforts. Working together under legal agreements, officers from these formations are responsible for supporting each other to ensure security at the Polish border during both wartime and peacetime.

Bibliography

Act of 4 September 2008 on the Protection of Shipping and Seaports, consolidated text: Journal of Laws 2024, item 597, Art. 27.

Act of 12 October 1990 on the Border Guard, consolidated text: Journal of Laws 2025, item 914, Arts. 11b–11d.

Antolak W., Tarapata S., Zontek W., *Przekroczenie granicy i pobyt na terytorium Polski imigrantów w warunkach stanu wyższej konieczności*, Kraków 2021.

Barszczewski W., Ciekanowski Z., Witkowicz S., *Specyfika działań Nadbużańskiego Oddziału Straży Granicznej dla zapewnienia bezpieczeństwa wschodniej granicy Unii Europejskiej*, Warszawa 2025.

Bieńkowska A., *Rola Straży Granicznej w kontekście funkcjonowania umów o małym ruchu granicznym. Casus pogranicza polsko-rosyjskiego*, Olsztyn 2023.

Bieńkowski K., *Ustawa o obronie Ojczyzny – zmiany w prawie wprowadzone po rosyjskiej inwazji na Ukrainę*, Warszawa 2022.

Blicharz, J., Znaczenie ekonomii społecznej jako narzędzie rozwoju społeczeństwa obywatelskiego w kontekście dostarczania usług publicznych. W: L. Zacharko (red.), *Nauka administracji. Paradygmaty współczesnego zarządzania w administracji publicznej* (s. 51–64). Racibórz: Wydawnictwo PWSZ w Raciborzu, 2016.

Błażejczak, K., Miejsce Straży Granicznej w systemie bezpieczeństwa państwa a typologia grup dyspozycyjnych. *Społeczeństwo i Polityka*, 3(68), 2021, 95–116.

Brunet-Jailly, E. *Borders and Bordering in the 21st Century*. Routledge, London 2022.

Celiński W., *Rola Straży Granicznej w systemie bezpieczeństwa narodowego*, Siedlce 2018.

Chochowski K., *Kryzys na granicy polsko-białoruskiej jako przejaw wojny hybrydowej. Aspekty administracyjnoprawne*, Tarnobrzeg 2021.

Chrostowska-Malak K., *Bezpieczeństwo i współpraca w polskiej polityce migracyjnej. Aspekty polityczne i prawne*, Warszawa 2022.

Ciechanowska J., Szwed K., *Odpowiedź Polski i Litwy na kryzys migracyjny przy granicy z Białorusią – próba porównania*, Rzeszów 2023.

Elak L., Oskierko M., Żurawski S., *Ochrona granicy polsko-białoruskiej w obliczu wojny hybrydowej*, Warszawa 2024.

European Court of Auditors, *Special Report 27/2022: Cross-border cooperation with neighbouring countries*. Luxembourg: Publications Office of the EU, 2022.

Fraszka B., *Sytuacja na granicy polsko-białoruskiej: przyczyny, aspekt geopolityczny, narracje*, Warszawa 2021.

Grajzer M., Żebrowski J., *Znaczenie Polski i polskiego zbrojenia dla bezpieczeństwa wschodniej flanki NATO*, Wrocław 2023.

Jakubczak, R., *Use of genocide by the Russian Federation in the conduct of hybrid activities and warfare in Ukraine*. Studia Prawnicze KUL, 4, 2024, 81–99.

Jurek K., *Działalność organizacji pozarządowych w kontekście kryzysu na granicy polsko-białoruskiej (2021–2022)*, Kraków 2022.

Kaczmarczyk B., *Uwarunkowania działania Straży Granicznej w kontekście współczesnych wyzwań i zagrożeń pozostających we właściwości tej formacji* [w:] *Globalne wyzwania i zagrożenia bezpieczeństwa międzynarodowego w XXI wieku*, Wrocław 2015.

Kitler, W., System ochrony państwa i jego porządku konstytucyjnego. *Wiedza Obronna*, Tom 268, Nr 3, 2019.

Kobus, I., *Straż Leśna w systemie bezpieczeństwa wewnętrznego* [Forest Guard in the internal security system]. Bezpieczeństwo. Teoria i Praktyka, 8(2), 2014, 51–61

Konieczny M., *Status, rola i zadania Straży Granicznej w Polsce*, Kraków 2021.

Kośka M., *Ochrona lądowej granicy Rzeczypospolitej Polskiej z Republiką Białorusi w związku z kryzysem migracyjnym w okresie od lipca 2021 roku do czerwca 2024 roku*, Piotrków Trybunalski 2024.

Kucińska N., *Analiza bezpieczeństwa Polski ze względu na sąsiedztwo Ukrainy*, Warszawa 2021.

Kuśmirek, K., *Information activities during the migration crisis on the Polish-Belarusian border as a threat to society's resilience*. Bezpieczeństwo. Teoria i Praktyka, 48(3), 2022, 311–321.

Lubimow J., *Współpraca transgraniczna Rzeczypospolitej Polskiej i państw postradzieckich w zakresie ochrony granic*, Gorzów Wielkopolski 2021.

Lubimow J., *Kryzys migracyjny na wschodniej granicy RP i jego znaczenia dla bezpieczeństwa strefy Schengen (granic wewnętrznych UE)*, Warszawa 2023.

Lubiewski P., *Granice Rzeczypospolitej Polskiej jako wyzwanie dla bezpieczeństwa państwa*, Przegląd Policyjny (nr specjalny), Warszawa 2019.

Leszczyńska K., *Poza granicami. Płeć społeczno-kulturowa w katolickich organizacjach migracyjnych*, Wydawnictwo Nomos, Kraków 2020.

Łuczaj K., *Migranci i uchodźcy w polskim dyskursie publicznym*, „Zagadnienia Społeczne", nr 1(15), Rzeszów 2021.

Moraczewska A., *Dychotomia działań Polski wobec imigrantów na granicach zewnętrznych Unii Europejskiej od 2021 roku*, Lublin 2023.

Mroczkowska K., *Prawna płaszczyzna zwalczania terroryzmu w Polsce*, Olsztyn 2024.

Niedźwiedzki D., *Kryzys humanitarny na granicy polsko-białoruskiej. Analiza zjawiska w perspektywie ładu społecznego*, Kraków 2024.

Nowak T., *Wzmacnianie bezpieczeństwa militarnego Polski na ścianie wschodniej*, Piotrków Trybunalski 2023.

Nowak D., *System ochrony granicy państwowej a sytuacja na granicy polsko-białoruskiej – zarys problematyki*, Rzeszów 2024.

Sójka W., Gąsiorek K., *Ochrona, obrona i bezpieczeństwo granicy państwowej w warunkach zewnętrznego zagrożenia państwa i w czasie wojny*, Warszawa 2021.

Ochyra, P., Brążkiewicz, D., Żurawski, S., & Ciekanowski, Z., *Siły Zbrojne RP jako element zarządzania kryzysowego w Polsce* [The Polish Armed Forces as an element of crisis management in Poland]. Studia Administracji i Bezpieczeństwa, 16(16), 2024, 291–307.

Olbrycht P., *Migracje na szlaku wschodnioeuropejskim jako potencjalne zagrożenie bezpieczeństwa Unii Europejskiej*, Wrocław 2021.

Orzech K., *Zagrożenia dla Polski kreowane przez Republikę Białorusi w kontekście sytuacji kryzysowej na granicy polsko-białoruskiej*, Warszawa 2021.

Płaczek, A., Policja i jej rola w ochronie granicy państwowej. *Przegląd Policyjny*, 29(nr specjalny), 2019, 87–97.

Regulation of the Council of Ministers of 31 August 2023 on cooperation between the Border Guard and units and subunits of the Polish Armed Forces, Journal of Laws 2023, item 1767.

Staniszewski R. M., *Uchodźcy czy migranci? – społeczna percepcja pojęć na podstawie wyników badań opinii publicznej*, Warszawa 2023.

Stańczuk I., *Konstytucyjny obowiązek ochrony granic RP w świetle kryzysu na granicy z Białorusią*, „Przegląd Prawa Konstytucyjnego", nr 3(67)/2022.

Stec, R., *Komentarz do art. 53* [w:] B. Rakoczy, A. Woźniak, & R. Stec (red.), Prawo łowieckie. Komentarz. LEX (SIP LEX), 2014.

Szczurek, T., Ministry of National Defense in the Crisis Management System. *Roczniki Nauk Społecznych*, 15(51)(2), 2023, 7–18.

Tkachuk O., *Znaczenie kryzysu migracyjnego na granicy polsko-białoruskiej dla polityki imigracyjnej i azylowej Unii Europejskiej*, „Wschodnioznawstwo", nr 16/2022.

Gąska, M., & Trubalska, J. (Red.)., *Bezpieczeństwo narodowe i międzynarodowe Rzeczypospolitej Polskiej: wybrane problemy*. Lublin: Innovatio Press, WSEI 2015.

Tutak G., *Polityka migracyjna Polski wobec zjawiska nielegalnej migracji. Przykład granicy polsko-białoruskiej*, „Rocznik Instytutu Europy Środkowo-Wschodniej", 22(4)/2024.

Tutak G., *Przeciwdziałanie nielegalnej imigracji do Polski na granicy polsko-ukraińskiej w latach 2009–2019*, „Nowa Polityka Wschodnia", nr 1(28)/2021.

Waksmundzka-Szarek M., Zalewski P., *Nielegalne działania cudzoziemców w procesie legalizacji pobytu w Polsce ze szczególnym uwzględnieniem województwa podkarpackiego. Analiza wybranych podatności i metod*, „Polityka i Społeczeństwo", 4(22)/2024.

Waniek, P., & Brążkiewicz, D., Kryzys migracyjny na granicy polsko-białoruskiej. W: D. Brążkiewicz, J. Nowicka, Z. Ciekanowski, & L. Elak (red.), *Współczesne wyzwania dla bezpieczeństwa państwa* (ss. 47–60). Wydawnictwo im. prof. Leszka J. Krzyżanowskiego, 2023.

Wawrzusiszyn A., *Kryzys migracyjny na granicy polsko-białoruskiej i jego wpływ na bezpieczeństwo Polski*, „Nowa Polityka Wschodnia", nr 2(33)/2022.

Wawrzusiszyn A., *Bezpieczeństwo wschodniej granicy Polski wobec współczesnych zagrożeń transgranicznych*, „Nowa Polityka Wschodnia", nr 3(38)/2023.

Wiśniewska K., *Straż Graniczna – organizacja i charakterystyka funkcjonowania na przykładzie Nadbużańskiego Oddziału Straży Granicznej*, „Zeszyty Naukowe WSEI. Administracja", 5(1)/2015.

Zamiar, Z., & Zamiar, P., Pozamilitarne ogniwa w systemie bezpieczeństwa militarnego państwa. *Zeszyty Naukowe Wyższej Szkoły Oficerskiej Wojsk Lądowych im. gen. T. Kościuszki*, *(4/162)*, 2011, 91–98.

Zyguła A., *Bezpieczeństwo wschodniej granicy Polski wobec aktualnych wyzwań i zagrożeń*, „Cybersecurity and Law", nr 2(10)/2023, s. 332–344.

About the Autors

Rafał Magoń – Major in the Polish Armed Forces, PhD student at WSB University in Dąbrowa Górnicza, specialist in automated command-and-control systems. His scientific interests focus on national and international security, in particular the role of uniformed services in ensuring the protection of the state border and the safety of the civilian population. In his research, he analyses the functioning of the military, police, and specialised formations in the context of hybrid threats, illegal migration, and crisis situations along the eastern border of the Republic of Poland. He combines practical military experience–including a four-month deployment with the Military Task Force "Podlasie" (WZZ "Podlasie") on Poland's eastern border–with academic research, developing solutions to strengthen the resilience and interoperability of security systems in both wartime and peacetime..

Paulina Polko – PhD, Assistant Professor at WSB University in Dąbrowa Górnicza, expert in internal security and public administration. She specialises in crisis management, migration policy, and the functioning of uniformed services in ensuring national security. Author of numerous scientific publications, she combines theoretical knowledge with practical experience in the field of public safety and security policy.

Damian Czapik, MA
WSB University in Dąbrowa Górnicza
damian.czapik@student.wsb.edu.pl
ORCID 0009-0001-7224-7462

DOI: 10.26410/SF_2/25/4

USING OPEN SOURCE INTELLIGENCE TO COMBAT HYBRID THREATS: REVIEW AND CASE STUDIES

Abstract

In the face of dynamic changes in the security environment and a growing number of hybrid activities, the role of white intelligence (OSINT) in identifying and countering these threats is becoming increasingly important. The article addresses the use of open sources of information in the processes of identifying, detecting, analysing, assessing and documenting activities of a hybrid nature, which may include disinformation, cyber attacks, social manipulation and, consequently, destabilisation of state structures. The definition and characteristics of hybrid threats and white intelligence are presented. In the course of the research, ten case studies of hybrid activities from the period 2013-2023 were analysed. The article concludes with a conclusion on the importance of white intelligence including the role of open sources of information in detecting and combating hybrid activities.

Keywords

Open-source intelligence, OSINT, hybrid threats, the role of information, security, information analysis

Introduction

In the modern world, threats are no longer exclusively in the form of conventional actions. They also take the form of hybrid actions. a threat in which a potential aggressor does not wear a uniform, flags of nationality or other identifying elements poses difficulties in terms of recognition and detection. Such a situation creates space for individual actors, groups of individuals and criminal or terrorist organisations to carry out activities aimed at destabilising public order, weakening state security structures and instilling fear in the public. In a hybrid threat environment, the line between peacetime and armed conflict becomes blurred. Hybrid threats can take various forms of influence including the form of, inter alia, a social media campaign seeking to create information chaos, in parallel with physical acts of terror. For this reason, the use of modern analytical tools, such as white intelligence sources and methods, which allow the identification of potential threats already at the stage of action planning by the adversary, becomes particularly important. Effective analysis of open sources of information is becoming a key element in countering modern hybrid threats.

There are no research studies in the literature that comprehensively address the use of white intelligence in identifying, detecting, analysing, documenting and countering all hybrid threats. One can only come across similar topics relating to the use of white intelligence in the identification of terrorist and cyber threats.

The paper aims to analyse and assess the extent to which white intelligence can become an important tool to identify and respond to hybrid threats. The sub-objectives of the paper include analysing and assessing real-life situations in which information obtained through white intelligence was involved in responding to hybrid threats.

The main research question is: *To what extent can white intelligence be an effective tool in identifying, analysing and countering hybrid threats?* The specific questions to the research question posed are: What forms of hybrid threats have occurred globally between 2013 and 2023? and What practical examples support the effectiveness of using OSINT in counter-hybrid operations?

This thesis is part of the security sciences research strand, particularly in the area of analysis of information security, the use of white intelligence and hybrid threats in the modern world.

An interdisciplinary approach was used to address the adopted research problem. Research methods such as the theoretical method, literature studies and content analysis of accounts and source materials were used in this study. The applied research methods made it possible to formulate conclusions on the role and significance of white intelligence as a tool supporting reconnaissance processes in the context of hybrid threats.

The research analysed ten case studies of hybrid actions from 2013-2023 (including the annexation of Crimea, the downing of flight MH17, Islamic State (IS/ISIS) actions around the world and the migration crisis on the Polish-Belarusian border). Secondary sources were used, including academic publications, reports from international institutions (e.g. Bellingcat, FBI, European Commission), press articles, studies by investigative journalists and social media data. a content analysis of white intelligence material was conducted to identify recurring patterns of counter-hybrid activity. For each incident, the source of the information, how it was used, the actors analysing it and the effect (including identification of perpetrators, international reactions, sanctions) were analysed. The methodological objective was to indicate to what extent white intelligence can act as an early warning tool and decision support in hybrid threat identification processes.

The study is preliminary and serves to initiate a broader discussion on the use of white intelligence in identifying hybrid threats.

White intelligence and hybrid threats

A hybrid threat is a situation in which an adversary (both state and non-state) uses diverse methods of action to achieve its objectives at the strategic level. It is characterised by combining political, military, economic, social and informational means with various forms of aggression, which may include conventional warfare, irregular action, terrorism, diversion or criminal activity[1]. Hybrid threats are defined identically by the European Union, where they are referred to as *a combination of repressive and subversive actions using conventional and unconventional methods (i.e. diplomatic, military, economic and technological) that can be used in a coordinated manner by state and non-state actors to achieve specific objectives, with actions below the threshold of officially declared war*[2]. Hybrid threats occur during hybrid operations resulting in hybrid warfare[3]. Hybrid activities include, but are not limited to: disinformation activities, propaganda activities, cyber-attacks (cyber-attacks), interference in political processes, imposition of economic pressure, instrumentalisation of irregular migration, state support of armed groups and hiring of mercenaries, intelligence operations of a diversionary and sabotage nature, terrorist activities and the use of chemical, biological, radiological and nuclear agents[4].

Due to the increasing complexity and ambiguity of hybrid threats, modern information-gathering methods that allow for their early identification and

1 *Encyklopedia bezpieczeństwa wewnętrznego*, A. Misiuk, J. Itrich-Drabarek, M. Dobwolska-Opała (ed.), Warsaw 2021, p. 295.

2 European Commission, *Joint Framework on countering hybrid threats a European Union response*, European Commission, Brussels 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016JC0018, (accessed: 26.06.2025).

3 B. Pacek, P. Pacek, *Psychologia wojny hybrydowej*, Warsaw-Siedlce 2019, p. 11.

4 F. Bryjka, *Rozwój unijnych zdolności do zwalczania zagrożeń hybrydowych*, „Strategic File", 9(117), 2022, p. 2.

counteraction are of particular importance. One important tool in this area is white intelligence, which enables the acquisition of a broad spectrum of information, the analysis of the information environment and the identification of potential threats before they take the form of open aggressive actions.

White intelligence[5] (open source interview) has the task of obtaining information from non-confidential as well as publicly available sources is also called OSINT (Open Source Intelligence). It is defined *as produced from publicly available information that is collected, used and disseminated over a specified period of time to appropriate audiences for specific intelligence needs*[6]. This type of information gathering is based on the use of open source tools[7] mainly obtained through observation or requests for access to information[8]. a hallmark of white intelligence is the obtaining of information using legitimate sources, which can be free as well as those that can be accessed for a fee. There is broad agreement among experts that the effort put into validation, analysis and dissemination in white intelligence distinguishes it from other types of information[9]. In the literature, white intelligence is also divided into passive and active reconnaissance activities[10]. Passive OSINT is observing the world, in this respect there is a lack of integration with the object of observation with whom one does not interact, making one an unobservable person. Active OSINT are activities that seek to interact with the object i.e. befriending the target e.g. commenting on posts to gain more information in an overt manner[11].

Hybrid threats pose a serious danger to the defence system of a state, including mainly its institutions and citizens. The reconnaissance potential of white intelligence is becoming an important means to counter and identify such threats.

Use of white intelligence and response to hybrid threats

White intelligence in responding to hybrid threats can be a significant preventive measure. In the context of reconnaissance and detection activities, OSINT can be used to analyse the flow of information from public media, which can facilitate the identification of the sources of dissemination of false information. It also allows a wide range of post-detection activities to identify the perpetrator. The value of white intelligence is that it can be used as circumstantial and evidentiary material.

5 A. Ziółkowska, *Open Source Intelligence (OSINT) as an element of military recon*, „Security and Defence Quarterly" 19/2, 2018, p. 69.

6 K. Wosiński, *Bezpieczeństwo osób i systemów IT z wykorzystaniem białego wywiadu*, Warsaw 2024, p. 11.

7 K. Wosiński, *OSINT: Nowy wymiar poszukiwań w sieci.*, Kraków 2024, p. 11.

8 K. Wosiński, *Bezpieczeństwo osób i systemów IT z wykorzystaniem białego wywiadu*, Warsaw 2024, p. 9.

9 D. V. Puyvelde, F. T. Rienzi, *The rise of open-source intelligence*, „European Journal of International Security" 2025, p. 4.

10 B. Terebiński, *OSINT vs. ensuring the security of legally protected information*, „Wiedza Obronna", vol. 287 no. 2/2024, p. 149.

11 D. Meredith, *The OSINT Handbook: a practical guide to gathering and analyzing online information*, 2024, p. 3.

Hybrid action detection is based on the early recognition of symptoms and signals indicating the possibility of threats, which may originate from both foreign states and non-state actors acting on their orders or on their own initiative, who may be motivated by radical views. Hybrid operations are characterised by multilayered and coordinated use of various means of social and informational influence.

In the early stages of detecting hybrid activity, white intelligence enables the collection of data from publicly available sources, which include news portals, social media, discussion forums, video platforms and apps through to public records. This makes it possible to quickly isolate anomalies in news narratives, identify organised disinformation campaigns and identify links between accounts responsible for creating and disseminating this content.

In this case, white intelligence makes it possible:

- a linguistic and semantic analysis of the message, which makes it possible to determine the source and purpose of the message,
- identifying the identities of fake creators and bots used to amplify propaganda messages,
- carrying out monitoring of social trends and sentiments and their background, so that potential escalations of social tensions can be forecast,
- mapping of networks between individuals, institutions and actors involved in content dissemination.

White intelligence can be a key enabler in this process, allowing information to be obtained from open sources in a legal and non-interfering manner. These can be used to augment operational or preventive actions. In the following, I have presented cases of the use of white intelligence in the field of counter-hybrid operations by referring to disclosed hybrid activities widely reported and analysed in the public and academic media.

Sketch 1. Cases of use of white intelligence in counter-hybrid operations

Hybrid threat	Time period	Description of the incident	Use of white intelligence	Effect of action
Terrorist attack during Boston marathon	April 2013	Improvised explosive device (IED) explosion at the finish line of the Boston Marathon. a sectarian terrorist attack carried out by two individuals (jihadists)[12].	Carrying out activities to search for the perpetrators of the attack through the use of amateur photographs and films and the image of likely perpetrators made available to the public[13]. Use of information obtained from social media in the course of an investigation[14].	Identification of the identity of the perpetrators of the attack through the released image of persons at the scene and the ongoing investigation carried out by the Federal Bureau of Investigation. Detention of the person responsible, the other died during the attempted arrest. Increased scrutiny of student visas[15].
The annexation of Crimea by the Russian Federation and the interference of the so-called "green men" on Ukrainian territory.	February/ March 2014	The encroachment on Ukrainian territory of unmarked and unidentified military units, uniformed without distinction or signs of national affiliation. The official narrative of the Russian Federation at the time was that there was no involvement in the conduct of these operations[16].	Carrying out activities in the course of analysing the uniforms and equipment of the attackers, establishing the location of the deployment of persons through metadata of photos and videos disseminated on the Internet. Recognition and identification of participating Russian soldiers on social media[17].	The disclosure that soldiers of the Russian Federation army and its forces and resources were behind the diversionary actions. Russia's hypocritical narrative has been revealed In view of the above, the imposition of sanctions through the European Union against the Russian Federation[18].

12 Państwowa Agencja Prasowa, *Dżochar Carnajew uznany za winnego zamachu w Bostonie*, https://wiadomosci.wp.pl/dzochar-carnajew-uznany-za-winnego-zamachu-w-bostonie-6025268084437633a, (accessed: 14.07.2025).

13 FBI, Boston Marathon Bombing, https://www.fbi.gov/history/famous-cases/boston-marathon-bombing, (accessed: 01.07.2025).

14 K. Wosiński, *O jeden OSINT za daleko, czyli przykre skutki złych analiz [Czwartki z OSINTem]*, https://sekurak.pl/o-jeden-osint-za-daleko-czyli-przykre-skutki-zlych-analiz-czwartki-z-osintem/, (accessed: 01.07.2025).

15 CNN, Skutki zamachu w Bostonie – ostrzejsze kontrole studentów, https://www.wprost.pl/swiat/398399/skutki-zamachu-w-bostonie-ostrzejsze-kontrole-studentow.html, (accessed: 14.07.2025).

16 M. Podraza, *Rosyjska aneksja ukraińskich terytoriów okupo*wanych w świetle prawa międzynarodowego, „Biuletyn Stowarzyszenia Absolwentów i Przyjaciół Wydziału Prawa Katolickiego Uniwersytetu Lubelskiego", t. XVIII, 20(2)/2023, pp. 221-222.

17 I. Ostanin, *Revealed: Around 40 Russian Troops from Pskov Died in the Ukraine, Reinforcement Sent In*, https://www.bellingcat.com/news/mena/2014/08/27/revealed-around-40-russian-troops-from-pskov-died-in-the-ukraine-reinforcement-sent-in, (accessed: 03.07.2025).

18 Rada Unii Europejskiej, Sankcje UE wobec Rosji – kalendarium, https://www.consilium.europa.eu/pl/policies/sanctions-against-russia/timeline-sanctions-against-russia, (accessed: 14.07.2025).

Hybrid threat	Time period	Description of the incident	Use of white intelligence	Effect of action
The downing of Malaysia Airlines flight 17 over Ukrainian territory.	July 2014	Shooting down of Malaysia Airlines plane over Ukraine in Donetsk region by Russians with 9K37 Buk missile launcher[19].	Implementation of activities through analysis of photos, movement of military equipment, testimonies of local residents, entry on Igor Girkin's VK platform[20] and its subsequent removal. Also using posts and videos on social media platforms.	Facts of the downing and the responsibility of the Russian Federation for the downing of the aircraft have been confirmed. Disclosure of this responsibility in investigations and international reports[21]. Imposition of sanctions on the Russian Federation[22].
IS / ISIS (Islamic State), online recruitment, propaganda and terrorist attacks[23].	2014 – 2020	Islamic State (IS/ISIS) propaganda efforts, recruitment of fighters through social media, fundraising and terrorist attacks[24].	Identification and tracking of sources in the form of recruitment channels, accounts and groups. Identification of links of people involved in ISIS recruitment[25]. Determination of geolocation data and identification of their links in the network[26]. Findings of institutions (foundations) supporting ISIS.	Closing down multiple channels of recruitment, foundations, establishing the identity of militants, detaining people linked to the Islamic State.
Russian disinformation campaign interfering in the election.	2016 – 2020	Information campaigns carried out using the method of disseminating disinformation ahead of the US election.	Analysis of metadata and IP sources, bot accounts and users of various platforms, as well as mapping and identifying sources of propaganda and disinformation narratives.	US Senate report revealing the influence structures of the Russian Federation and the influence of trolls (e.g. IRA)[27].

19 E. Higgins, The Buk That C*ould – An Open Source Odyssey*, https://www.bellingcat.com/news/uk-and-europe/2014/07/28/the-buk-that-could-an-open-source-odyssey, (accessed: 04.07.2025).

20 TŁ., Europejski trybunał: Rosja stoi za zestrzeleniem pasażerskiego boeinga, https://www.tvp.info/87748630/katastrofa-samolotu-malaysia-airlines-mh17-europejski-trybunal-praw-czlowieka-etpcz-to-rosja-odpowiada-za-zestrzelenie-pasazerskiego-samolotu-malaysia-airlines-mh17, (accessed: 03.07.2025).

21 A. Holligan, K. Vandy, *MH17: Three guilty as court finds Russia-controlled group downed airliner*, https://www.bbc.com/news/world-europe-63637625, (accessed: 14.07.2025).

22 Council of the European Union, Foreign Affairs Council , 22 July 2014, https://www.consilium.europa.eu/en/meetings/fac/2014/07/22, (accessed: 14.07.2025).

23 O. Reczko, *OSINT – otwarte źródła w walce z z*agrożeniami, https://rynekinformacji.pl/osint-przy-wykrywaniu-zamachowca-w-usa/, (accessed: 04.07.2025).

24 A. Badawy, E. Ferrara, *The Rise of Jihadist Propaganda on Social Networks*, „Journal of Computational Social Science", 2018, p. 11.

25 M. M. Robinson, *Social media recruitment and online propaganda by extremist groups*, University of Northern Iowa 2022, https://scholarworks.uni.edu/cgi/viewcontent.cgi?article=1540&context=hpt, (accessed: 06.07.2025).

26 M. Lakomy, *Internet w działalnośći tzw. Państwa Islamskiego: nowa jakość cyberdżihadyzmu?*, „Studia Politologiczne", 2015, p. 159.

27 *Repor tof the select committee on intelligence United States Senate on russian active measures campaigns and interference in the 2*016 U.S. election volume 2: russia's use of social media with additional views, https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-documents-report-volume2.pdf, (accessed: 08.07.2025).

Hybrid threat	Time period	Description of the incident	Use of white intelligence	Effect of action
Syria to identify responsibility in war crimes committed against civilians.	March/ April 2017	Publication of social media footage of the use of chemical weapons by armed forces against civilians. Activities carried out by the Assad regime The regime of Bashar al-Assad.	Geolocation of video footage, analysis of images of bomb debris and flight trajectories, and drawing on metadata. Analysis of evidence of the occurrence from public and social media.	The results of the investigations provided evidence against the regime of Bashar al-Assad. The Bellingcat organisation (which specialises in OSINT investigations) confirmed the use of SARIN battle gas from the air[28].
Wagner Group in Africa.	2020 – 2023	Support by Wagner Group mercenaries (Russian private military company) of instability and local conflicts in, among others, the Central African Republic, Mali, Sudan and Libya (Sahel and North West Africa Region).	Monitoring the presence of the Wagner group through geolocalisation analyses[29], photographs and films and satellite distribution. Tracing sources and propaganda narratives and links of associated individuals. Documenting crimes and warfare.	Determining in which countries the Wagner Group operates. Identifying commanders, members and their connections. The occurrence of international pressure[30] and sanctions[31].
Rioting and an attack on the US Capitol.	January 2021	Using social media to plan and organise a march on Capitol Hill[32].	Identification of participants and instigators of the riots by analysis of photographs and recordings[33]. Documenting and archiving digital evidence. Use of white intelligence sources as evidence.	Disclosure of identity of rioters. Arrests and indictments following identification of persons[34].

28 E. Higgins, *The OPCW Fact Finding Mission Confirms More Sa*rin and Chlorine Use in Syria, https://www.bellingcat.com/news/mena/2018/06/13/opcw-fact-finding-mission-confirms-sarin-chlorine-use-syria/, (accessed: 08.07.2025).

29 ADDO, Video Stars: Russia's viral video propaganda in Africa, https://disinfo.africa/video-stars-russias-viral-video-propaganda-in-africa-2663403a85f0, (accessed: 16.07.2025).

30 S. Magdy, *US seeks to expel Russian mercenaries from Sudan, Libya*, https://apnews.com/article/russia-ukraine-putin-politics-libya-government-b4218ab0163e6c5e271a3902cd893759, (accessed: 09.07.2025).

31 DW, *EU sanction*s Russian Wagner Group for African operations, https://www.dw.com/en/eu-sanctions-russian-wagner-group-for-african-operations/a-64822435?, (accessed: 09.07.2025).

32 P. Czajkowski, FBI: Atak na Kapitol nie był planowany w mediach społecznościowych. Brak dowodów na udział Trumpa, https://ithardware.pl/aktualnosci/fbi_atak_na_kapitol_nie_byl_planowany_w_mediach_spolecznosciowych_brak_dowodow_na_udzial_trumpa-17533.html, (accessed: 09.07.2025).

33 M. Burgess, Open-source sleuths are already unmasking the Capitol Hil*l mob*, https://www.wired.com/story/capitol-riot-photos-video-online/, (accessed: 10.07.2025).

34 G. Myre, How Online Sleuths Identified Rioters At The Capitol, https://www.npr.org/2021/01/11/955513539/how-online-sleuths-identified-rioters-at-the-capitol, (accessed: 10.07.2025).

Hybrid threat	Time period	Description of the incident	Use of white intelligence	Effect of action
Start of the migration crisis on the Polish-Belarusian border (EU border and Schengen area)	2021	Hybrid actions with the use of migrants on the Polish-Belarusian border. Disinformation and illegal crossing of the Polish State border[35] including the Schengen Area.	Monitoring of foreign accounts, analysis of videos, photos and posts made on social media. Analysis of foreign media information. Analysis of metastasis channels. Verification of disinformation content.	Blocking some of the channels of transit[36], unmasking the disinformation campaign[37], and identifying points of transit and places of concentration of migrants.
Russian Federation's military invasion of Ukrainian territory.	February 2022	Early detection of movements and dislocation of Russian troops prior to invasion. Accumulation of troops near the border from autumn 2021[38] , in the official media coverage under the pretext of a military exercise entitled Zapad-2021.	Analysis of satellite imagery[39], soldiers' posts and video footage and photos on social media. Identification of equipment, equipment and combat units. Mapping of warfare by updating troop movements, frontline maps and equipment losses. Tracking official and unofficial reports on warfare. Identification and documentation of war crimes (e.g. Bucza)[40].	International warning and defence preparedness. Evidence from white intelligence sources was used by NATO member states and the EU as factual evidence of the invasion and war crimes[41].

Source: own elaboration.

The above examples illustrate that white intelligence is widely applicable to hybrid threat operations. It is a valuable tool and source of information. Its application has a bearing on the outcome of hybrid threat operations. OSINT is an important element in recognising, identifying, analysing and documenting such threats.

35 O. Filipec, *Multilevel Analysis of the 2021 Poland-Belarus Border Crisis in the Context of Hybrid Threat*s, „Central European Journal of Politics", Vol. 8(1)/2022, pp. 2–3.

36 M. Scislowska, Y. Karmanau, *Why tensions have been growing along NATO's eastern border with Belarus*, https://apnews.com/article/nato-poland-belarus-wagner-migrants-explainer-aad1f9d81ce9eaed2fed0d6128fa528d, (accessed: 11.07.2025).

37 M. D. Weiss, M. Richter, *How a Manufactured Mi*grant Crisis Showed That Europe's Last Dictator Can Rattle the E.U., https://time.com/6121141/belarus-europe-migrants, (accessed: 11.07.2025).

38 Planet (SkySat), *The Most D*ocumented Invasion In History, www.planet.com/ukraine-photo-story/, (accessed: 17.07.2025).

39 M. Meaker, *High* Above Ukraine, Satellites Get Embroiled in the War, www.wired.com/story/ukraine-russia-satellites/, (accessed: 11.07.2025).

40 E. Higgins, *Russia's Bucha 'Facts' Versus the Evidence*, https://www.bellingcat.com/news/2022/04/04/russias-bucha-facts-versus-the-evidence, (accessed: 17.07.2025).

41 V. Elliott, *The US Plan to Document War Crimes in Ukraine*, www.wired.com/story/conflict-observatory-ukraine-russia-war-crimes/, (accessed: 17.07.2025).

Regardless of the type of hybrid threats present, white intelligence provides the tools and means to:

- responding dynamically to incidents by promptly analysing publicly available material and sources, particularly from social media (e.g. photos, videos, posts, geolocalisation data and metadata) and live streaming services (e.g. YouTube, Snap, Instagram, Twitch). Observation of sources enables correlations of information reliability.
- update and verify information particularly related to crisis situations through real-time tracking of, inter alia, live reports, journalistic coverage, satellite image viewing and social media monitoring, as well as information provided by whistleblowers.
- support decision-making and analytical processes at tactical, operational and also strategic levels,
- secure and familiarise themselves with evidence that can be used in investigative activities and to draw consequences for perpetrators of hybrid activities.

In view of the above, it can be concluded that the development of competencies in the use of white intelligence and the systemic implementation and framing in the field of state security of such tools as part of the practice of recognising, identifying and documenting crime and hybrid threats is applicable.

In order to effectively use white intelligence in the role of identifying and responding to hybrid threats, it is necessary to apply an algorithm of activities, the application of which can translate into effective detection, circumstantial and evidentiary actions.

Sketch 2. Algorithm of white intelligence activities in countering hybrid threats.

Stage of action	Activities with OSINT	Achievable effects
Detection (disclosure)	Monitoring of forums, social media including groups, communities, organisations and public information sources. Analysis of social trends and identification of anomalies. Revealing indications of possible hybrid threats.	This action enables early warning (prevention) and preparation of a response to the possible occurrence of hybrid threats. It also enables a rapid response to threats that already exist.
Hazard analysis (risk assessment)	Threat analysis through visualisation of information sources including identification of links between people, groups, communities, places and things. It enables a comprehensive picture of the situation and the identification of potential threats and better decision-making.	This activity makes it possible to identify external and internal influence structures, analyse the intentions, motives and purpose of the activity including risk levelling. This activity makes it possible to identify key actors and assess the potential impact of their activity on national security.

Stage of action	Activities with OSINT	Achievable effects
Verification of facts (reliability of information)	Confrontation with other sources of information from individuals, institutions, organisations through the public media into the scope which includes open source information. Allows for findings on targeted evidentiary and circumstantial issues. Analysis of the credibility of information and possible threats. Enables verifying the true version of events, identifying discrepancies, and building a coherent and credible picture of the situation.	Act by separating false from true information. Establishing the credibility of information sources and facts. Prioritising action resulting in effective information management. Acting to minimise the risk of disinformation.
Reporting (documenting)	Creation of reports by whistleblowers and reports addressed to national security services. Transmission of verified information. Documenting material by securing it for future evidence or background information.	Action through whistleblowers to support services for targeted action. Enables effective prioritisation of threats and optimisation of the response process. Action by securing digital traces and securing evidence.

Source: own elaboration.

The steps indicated provide a structured model for the use of white intelligence in countering hybrid threats. The application of this algorithm can enable the effectiveness of security services to be increased. The coordinated use of these stages makes it possible to treat white intelligence not only as a tool supporting detection activities and response to hybrid threats, but as a fully-fledged element of the state security system.

Summary

Contemporary hybrid threats, are characterised by multidimensionality and irregularity. It involves the integration of military, informational and psychological activities. White intelligence is gaining importance as a tool with significant action in terms of detection, prevention, analysis and response to such challenges. The examples in the research analysis presented here confirm the effectiveness of this type of action. White intelligence enables the collection of information from open sources, including primarily social media, websites, public records or satellite imagery. The use of this intelligence method results in the possibility to identify perpetrators (including crimes, disinformation and terrorist attacks), influence structures (external and internal) and sources of information distribution. OSINT also makes it possible to secure evidence that can be used in domestic and foreign proceedings.

The area and effectiveness of the use of white intelligence indicates that it should be permanently integrated into the state security system and participate in the

identification and counteraction of hybrid threats. The examples presented in the research paper indicate that the cooperation of services with the public through the exchange of information is significant in order to increase the effectiveness of detection and neutralisation of existing hybrid threats (sharing of images and photographs and recordings seeking to identify the perpetrators). The reliability of open-source information is based on its verification, which has the effect of preventing disinformation, particularly in a changing and computerised environment. The examples shown indicate that white intelligence, through the documentation and archiving of information, has evidentiary as well as operational significance.

An algorithm for countering hybrid threats using white intelligence, based on early detection (disclosure), threat analysis (risk assessment), fact verification (information credibility) and reporting (documentation), provides a structured approach to the use of white intelligence in the practice of whistleblowers and state security services.

Bibliography

ADDO, *Video Stars: Russia's viral video propaganda in Africa*,

https://disinfo.africa/video-stars-russias-viral-video-propaganda-in-africa- 2663403a85f0

Badawy A., Ferrara E., *The Rise of Jihadist Propaganda on Social Networks*, „Journal of Computational Social Science" 2018.

Bryjka F., *Rozwój unijnych zdolności do zwalczania zagrożeń hybrydowych,* „Strategic File", 9(117)/2022.

Burgess M., *Open-source sleuths are already unmasking the Capitol Hill mob*, https://www.wired.com/story/capitol-riot-photos-video-online/.

CNN, *Skutki zamachu w Bostonie – ostrzejsze kontrole studentów*, https://www.wprost.pl/swiat/398399/skutki-zamachu-w-bostonie-ostrzejsze- kontrole-studentow.html.

Council of the European Union, *Foreign Affairs Council*, https://www.consilium.europa.eu/en/meetings/fac/2014/07/22

Czajkowski P., *FBI: Atak na Kapitol nie był planowany w mediach społecznościowych. Brak dowodów na udział Trumpa,* https://ithardware.pl/aktualnosci/fbi_atak_na_kapitol_nie_byl_planowany_w_

mediach_spolecznosciowych_brak_dowodow_na_udzial_trumpa-17533.html

DW, *EU sanctions Russian Wagner Group for African operations*,

https://www.dw.com/en/eu-sanctions-russian-wagner-group-for-african- operations/a-64822435?

Encyklopedia bezpieczeństwa wewnętrznego, Misiuk A., Itrich-Drabarek J., Dobwolska-Opała M. (ed.), Warsaw 2021.

Elliott V., *The US Plan to Document War Crimes in Ukraine*, www.wired.com/story/conflict-observatory-ukraine-russia-war-crimes/

European Commission, *Joint Framework on countering hybrid threats a European Union response*, European Commission, Brussels 2016,

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016JC0018.

FBI, *Boston Marathon Bombing*,

https://www.fbi.gov/history/famous-cases/boston-marathon-bombing

Filipec O., *Multilevel Analysis of the 2021 Poland-Belarus Border Crisis in the Context of Hybrid Threat*s, „Central European Journal of Politics", Vol. 8(1)/2022, pp. 1-18.

Higgins E., *Russia's Bucha 'Facts' Versus the Evidence*, https://www.bellingcat.com/news/2022/04/04/russias-bucha-facts-versus-the- evidence

Higgins E., *The Buk That Could – An Open Source Odyssey*, https://www.bellingcat.com/news/uk-and-europe/2014/07/28/the-buk-that-could- an-open-source-odyssey

Higgins E., *The OPCW Fact Finding Mission Confirms More Sarin and Chlorine Use in Syria*, https://www.bellingcat.com/news/mena/2018/06/13/opcw-fact-finding-mission-confirms-sarin-chlorine-use-syria/

Holligan A., Vandy K., *MH17: Three guilty as court finds Russia-controlled group downed airliner*, https://www.bbc.com/news/world-europe-63637625

Kuciel D., *OSINT sztuka zdobywania informacji*, 2023.

Lakomy M., *Internet w działalności tzw. Państwa Islamskiego: nowa jakość cyberdżihadyzmu?*, „Studia Politologiczne", 2015, p.156-184.

Magdy S., *US seeks to expel Russian mercenaries from Sudan, Libya*, https://apnews.com/article/russia-ukraine-putin-politics-libya-government-b4218ab0163e6c5e271a3902cd893759

Meaker M., *High Above Ukraine, Satellites Get Embroiled in the War*, www.wired.com/story/ukraine-russia-satellites/

Meredith D., *The OSINT Handbook: a practical guide to gathering and analyzing online information*, 2024.

Myre G., *How Online Sleuths Identified Rioters At The Capitol*, https://www.npr.org/2021/01/11/955513539/how-online-sleuths-identified-rioters-at-the-capitol

Ostanin I., *Revealed: Around 40 Russian Troops from Pskov Died in the Ukraine*, *Reinforcement Sent In*,

https://www.bellingcat.com/news/mena/2014/08/27/revealed-around-40-russian-troops-from-pskov-died-in-the-ukraine-reinforcement-sent-in

Pacek B., Pacek P., *Psychologia wojny hybrydowej*, Warsaw-Siedlce 2019.

Państwowa Agencja Prasowa, *Dżochar Carnajew uznany za winnego zamachu w Bostonie*, https://wiadomosci.wp.pl/dzochar-carnajew-uznany-za-winnego-zamachu-w-bostonie6025268084437633a

Podraza M., *Rosyjska aneksja ukraińskich terytoriów okupowanych w świetle prawa międzynarodowego*, „Biuletyn Stowarzyszenia Absolwentów i Przyjaciół Wydziału Prawa Katolickiego Uniwersytetu Lubelskiego" t. t. XVIII, 20(2)/2023 pp. 219-233.

Planet (SkySat), *The Most Documented Invasion In History*,

www.planet.com/ukraine-photo-story/

Puyvelde D. V., Rienzi F. T., *The rise of open-source intelligence*, „European Journal of International Security" 2025.

Rada Unii Europejskiej, *Sankcje UE wobec Rosji – kalendarium*, https://www.consilium.europa.eu/pl/policies/sanctions-against-russia/timeline-sanctions-against-russia

Reczko O., *OSINT – otwarte źródła w walce z zagrożeniami*, https://rynekinformacji.pl/osint-przy-wykrywaniu-zamachowca-w-usa/

Report of the select committee on intelligence United States Senate on russian active measures campaigns and interference in the 2016 u.s. election ' volume 2: russia's use of social media with additional views,

https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-documents-report-volume2.pdf

Robinson M.M., *Social media recruitment and online propaganda by extremist groups*, University of Northern Iowa 2022,

https://scholarworks.uni.edu/cgi/viewcontent.cgi?article=1540&context=hpt

Scislowska M., Karmanau Y., *Why tensions have been growing along NATO's eastern border with Belarus*, https://apnews.com/article/nato-poland-belarus-wagner-migrants-explainer-aad1f-9d81ce9eaed2fed0d6128fa528d

Terebiński B., *OSINT vs. ensuring the security of legally protected information*, „Wiedza Obronna", vol. 287 no. 2/2024, p. 142-157.

TŁ., *Europejski trybunał: Rosja stoi za zestrzeleniem pasażerskiego boeinga*, https://www.tvp.info/87748630/katastrofa-samolotu-malaysia-airlines-mh17europejski-trybunal-praw-czlowieka-etpcz-to-rosja-odpowiada-za-zestrzelenie-pasazerskiego-samolotu-malaysia-airlines-mh17

Weiss M.D., Richter M., *How a Manufactured Migrant Crisis Showed That Europe's Last Dictator Can Rattle the E.U*, https://time.com/6121141/belarus-europe-migrants

Wosiński K., *Bezpieczeństwo osób i systemów IT z wykorzystaniem białego wywiadu*, Warsaw 2024.

Wosiński K., *O jeden OSINT za daleko, czyli przykre skutki złych analiz [Czwartki z OSINTem]*, https://sekurak.pl/o-jeden-osint-za-daleko-czyli-przykre-skutki-zlych-analiz-czwartki-z-osintem/

Wosiński K., *OSINT: Nowy wymiar poszukiwań w sieci*, Kraków 2024.

Ziółkowska A., *Open Source Intelligence (OSINT) as an element of military recon*, „Security and Defence Quarterly" 19/2, 2018, p. 65-77.

About the Author:

Damian Czapik – master's degree in national security and history at the John Paul II Catholic University of Lublin. Student of the doctoral seminar in the discipline of security sciences at the WSB Academy in Dąbrowa Górnicza. Research interests: the role of information in society, information security, the social and military aspect of military operations, and the use of intelligence methods to ensure security.

Lukasz Mileszko, MPhil
WSB University in Dąbrowa Górnicza
e-mail: lukaszmileszko@gmail.com
ORCID: 0009-0000-3283-4243

DOI: 10.26410/SF_2/25/5

SHACKLED THE CONTEMPORARY FACE OF HUMAN TRAFFICKING

Abstract

The paper examines the present form of human trafficking, thus the contemporary face of modern slavery, including its legal aspects, various forms, examples, methods of exploitation employed by perpetrators, the geopolitical factors that shape its scale and scope, as well as the efforts and problems of the organizations working to reduce the global impact of this phenomena and also the efficiency of the countermeasures used against human trafficking on national and international levels. Author uses material and analysis, from organisations such as: UNHCR – *United Nations High Commissioner for Refugees*. IOM – *International Organization for Migration*, Europol – *European Union Agency for Law Enforcement Cooperation*, Interpol – *International Criminal Police Organization* ICC – International Criminal Court, U.S. Department of State information and other non-governmental organisation – NGO's.

Keywords

human trafficking, crime, security, armed conflict, force labour, sexual exploitation, children trafficking, children exploitation, organ trafficking, illegal international adoption

Introduction

The history of human trafficking dates back to ancient times, when slavery was a widely accepted economic and social practice. Ancient Rome, Greece, and Egypt operated on the basis of slave labour, with people treated as commodities; bought, sold, and inherited. In the Middle Ages, the slave trade became more institutionalized, and with the colonial expansion of Europeans, this phenomenon acquired a global dimension, exemplified by the transatlantic slave trade of the 16th–19th centuries, which primarily involved Africans being transported to the Americas.[1] It was only in the 19th century that systematic efforts to abolish slavery began. The slave trade was banned (Great Britain in 1807),[2] and slavery itself was prohibited (the United States in 1865 with the 13th Amendment to the U.S. Constitution).[3] Despite these steps, the phenomenon did not disappear the forms, terminology, and mechanisms changed, evolving to adapt to new realities. This is clearly visible in the modern aspect of human trafficking, which in many ways continues the old model of exploitation, adjusting it to global capitalism, illegal migration, and the organized crime associated with it.[4] In developed countries, it takes on more subtle forms for example; forced labour in the service sector, domestic care, or construction. In contrast, in states with unstable political or economic situations, such as those affected by armed conflicts, human trafficking often takes the form of organized exploitation of civilians by paramilitary groups, smugglers, criminal organizations, and even official state structures. According to the Global Slavery Index 2023, around 50 million people worldwide are affected by problem of the modern human trafficking.[5] Every 30 seconds someone becomes a victim of it, it generates an annual turnover of $150 – 250 billion, that's equivalent to 3 times the GDP of a medium-sized European country.[6,7] The occurrence is one of the most severe violations of human rights, remaining a global issue with a complex and dynamic nature, depriving its victims of freedom, dignity, and fundamental rights. The definition of human trafficking was precisely established in the Palermo Protocol (2000), which supplements the United Nations Convention against Transnational Organized Crime. According to this protocol, human trafficking is defined as: "the recruitment, transportation, transfer, harbouring or receipt of persons, by means of threat, use of force, coercion, abduction, fraud, deception, abuse of power or a position of vulnerability, for the purpose of exploitation," including but not limited to prostitution, forced labour, or slavery.[8] The issue

1 D. Eltis, *The Rise of African Slavery in the Americas*, Cambridge University Press, 2000, p. 1.

2 *An Act for the Abolition of the Slave Trade* (47 Geo. III Sess. 1 c. 36).

3 *Thirteenth Amendment to the United States Constitution*.

4 K. Bales, *Disposable People: New Slavery in the Global Economy*, University of California Press, 2004, p. 7.

5 *Global Slavery Index, Walk Free Foundation*, 2023. https://www.walkfree.org/global-slavery-index/ accessed 14 Oct. 2025

6 *Mariposa, 2019*. https://www.mariposacenter.org/blog/every-30-seconds-another-person-becomes-a-victim-of-human-trafficking/ accessed 14 Oct. 2025

7 *Worldomete, 2023*. https://www.worldometers.info/gdp/gdp-by-country/ accessed 14 Oct. 2025

8 United Nations Convention against Transnational Organized Crime, *Palermo Protocol*, 2000.

of human trafficking falls within the broader framework of human rights, migration law, and social rights, and its eradication requires international cooperation and comprehensive measures.

Material and methods used for research

The research process of theoretical aspects for this material used analysis, inference, data analysis and the author's observations, data from organisations as: UNHCR – *United Nations High Commissioner for Refugees*. IOM – *International Organization for Migration*, Europol – *European Union Agency for Law Enforcement Cooperation*, Interpol – *International Criminal Police Organization* ICC – International Criminal Court, U.S. Department of State information and other non-governmental organisation – NGO's.

Legal repercussions U.S. vs Europe

In the U.S., human trafficking is prosecuted under the Trafficking Victims Protection Act (TVPA) and various federal and state laws. It covers both sex trafficking and labour trafficking, including forced labour, debt bondage, and exploitation of minors. Penalties for trafficking are severe. a person convicted of trafficking adults may face up to 20 years in federal prison, and if the trafficking involves aggravating circumstances (e.g. kidnapping, sexual abuse, or death), the sentence may increase to life imprisonment. For child trafficking, the penalty can also include a minimum of 15 years up to life.[9] Convicted traffickers may also face fines, asset forfeiture, and mandatory restitution to victims. However, prosecution is challenging. Human trafficking is often hidden, victims are afraid or unwilling to testify, and traffickers use complex methods to evade law enforcement. According to U.S. Department of Justice reports, although hundreds of trafficking cases are prosecuted annually, conviction rates remain relatively low compared to the estimated scale of trafficking.[10] In addition, many cases are prosecuted under related charges (e.g., kidnapping, rape, immigration violations) rather than trafficking per se, due to evidentiary issues.

In the European Union, human trafficking is criminalized under Directive 2011/36/EU, which mandates all member states to penalize trafficking with effective, proportionate, and dissuasive penalties, including a minimum of 5 years imprisonment, and 10 years or more for aggravated offenses (such as those involving children, organized crime, or severe exploitation).[11]

9 *18 U.S. Code*. Article 1589, 1584, 1590

10 *National Institute of Justice, 2020.* https://nij.ojp.gov/topics/articles/gaps-reporting-human-trafficking-incidents-result-significant-undercounting accessed 14 Oct. 2025

11 *Directive 2011/36/EU of the European Parliament and of the Council*

Each EU member state enforces its own laws.

- Germany: under 1 up to 10 years, with harsher sentences if minors are involved.[12]
- France: Up to 20 years' imprisonment and significant fines.[13]
- Poland: 3 to 15 years for trafficking-related crimes.[14]
- Netherlands: from 6 to 15 years for aggravating factors.[15]

Conviction remains difficult across Europe. The European Commission and Europol have noted systemic underreporting, difficulties in identifying victims, limited cooperation across borders, and insufficient training of frontline professionals. Although all EU countries have legal frameworks in place, enforcement varies significantly. In 2022, Eurostat data revealed that only around 30% of registered suspects in trafficking cases across the EU were eventually convicted, and the conviction rate for cross-border trafficking was even lower.[16] Both the U.S. and the EU have strong legal frameworks against human trafficking, with potential sentences ranging from 5 years in EU to life imprisonment in US, depending on severity. Nonetheless, prosecution remains difficult, often due to the hidden nature of trafficking, lack of victim cooperation, and complex transnational operations. Improving identification, victim support, and international cooperation remains essential to increasing conviction rates and combating trafficking effectively.

Modern forms of human trafficking

Forced Labor

One of the most common forms of human trafficking is forced labour, which occurs in agriculture, construction, industrial or domestic environment, and the fishing sector. Victims are forced to work under threats of violence, confiscation of documents, debt bondage, or other forms of coercion.

Sexual Exploitation

The most recognizable and widely publicized form of human trafficking is sexual exploitation, which includes forced prostitution, child pornography, and trafficking of women for so-called forced or polygamous marriages. Victims are often subjected to physical and psychological abuse, and their rights are completely disregarded.

Exploitation of Children

Children are especially vulnerable to trafficking for various purposes – including labour, sexual exploitation, begging, or even as soldiers or slaves in armed conflicts. In some parts of the world, child trafficking for organ removal is also a serious issue.

12 *German Criminal Code*. Strafgesetzbuch StGB. Section 232

13 *French Penal Code*. Article 225-4-1,2,3

14 *Polish Penal Code*. Article 189a-1

15 *Dutch Criminal Code*. Article 273-F

16 *European Commission, 2024.* https://home-affairs.ec.europa.eu/news/newly-released-data-show-increase-trafficking-human-beings-2024-02-28_en accessed 14 Oct. 2025

Organ Trafficking

Organ trafficking is one of the most brutal forms of exploitation, where victims – often poor or homeless or from underdevelopment countries – are coerced or deceived into giving up their organs for the black market. Transplants involving organs obtained in this way take place in many countries and represent a serious violation of medical ethics.

Other Forms

Other forms of human trafficking include forcing victims to commit crimes, trafficking related to armed conflict, and trafficking for illegal international adoption.

Methods used by perpetrators

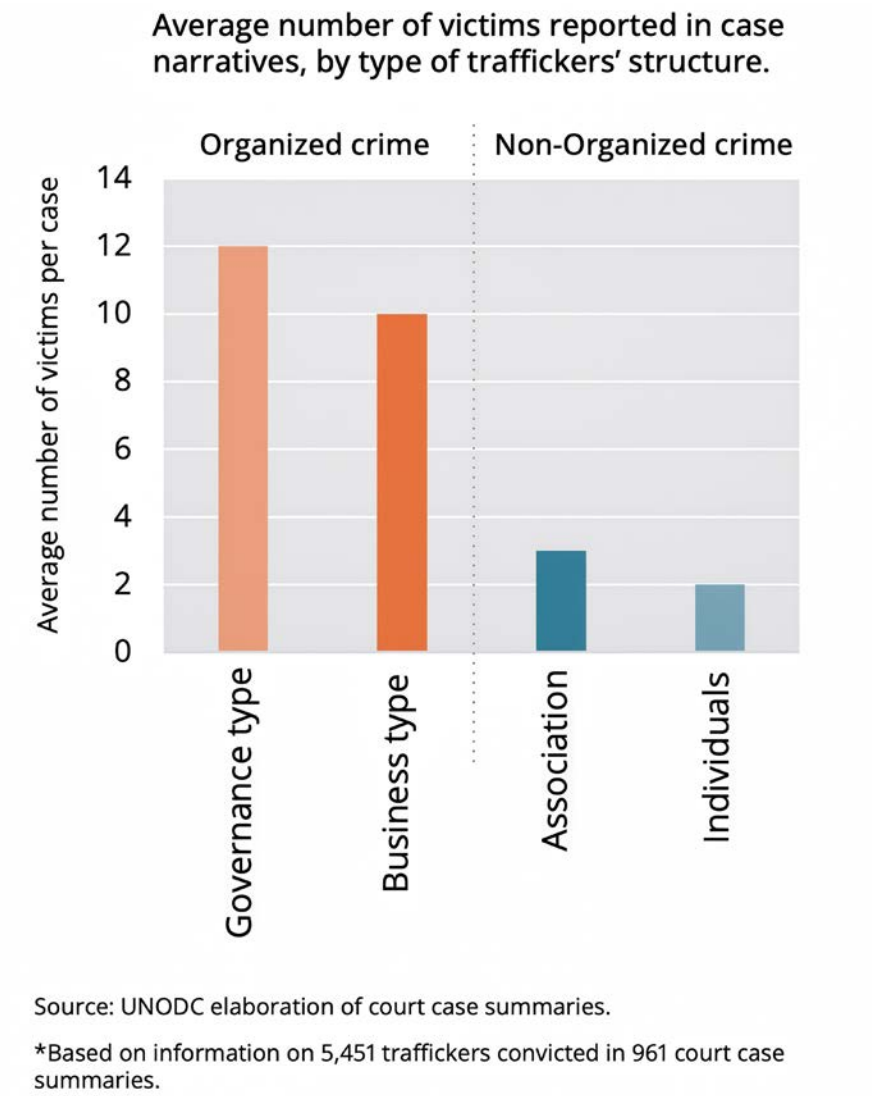
Perpetrators of human trafficking employ a variety of techniques for recruiting, controlling, and exploiting victims. Modern technologies have significantly facilitated their activities. Recruitment often takes place under the pretext of legitimate employment, education, or improving one's living conditions. Offenders exploit the trust of victims and their families, as well as their difficult economic and social circumstances. Common methods include fake job advertisements, fraudulent employment agencies, and the use of social media. Once the victim has been recruited, perpetrators use physical and psychological violence, threats, confiscation of identity documents, and social isolation. Victims are often made dependent on the traffickers for long periods, with their sense of hopelessness deepened by the lack of access to assistance. The internet and modern technologies, social platforms, encrypted communication tools, dark web and globalisation enable criminals to communicate more easily, recruit online, and monitor and control victims to execute criminal activities and exploitation.

Geopolitical conditions shaping human trafficking

The political and economic situation worldwide has a significant impact on the scale and nature of human trafficking. Conflicts such as the war in Ukraine, has caused a mass displacement of people, increasing the risk of human trafficking practice, particularly involving women and children. Since the outbreak of the full-scale war in 2022, serious concerns have arisen regarding the forced relocation and deportation of Ukrainian children to the Russian Federation and occupied territories. According to Ukrainian authorities and international organizations, thousands of children particularly from orphanages, care homes, and conflict zones have been taken without consent and relocated under the pretext of evacuation, protection, or adoption to Russia motherland. In 2023, the International Criminal Court (ICC) issued arrest warrants for Russian President Vladimir Putin and Children's Rights Commissioner Maria Lvova-Belova, accusing them of unlawfully deporting children

from Ukrainian territories. Russia has denied wrongdoing, framing the transfers as humanitarian aid.[17] The scale of this event is under ongoing investigation and requires further research however some sources indicated the number of 20.000 thousands victims involved.[18]

Chart No. 1



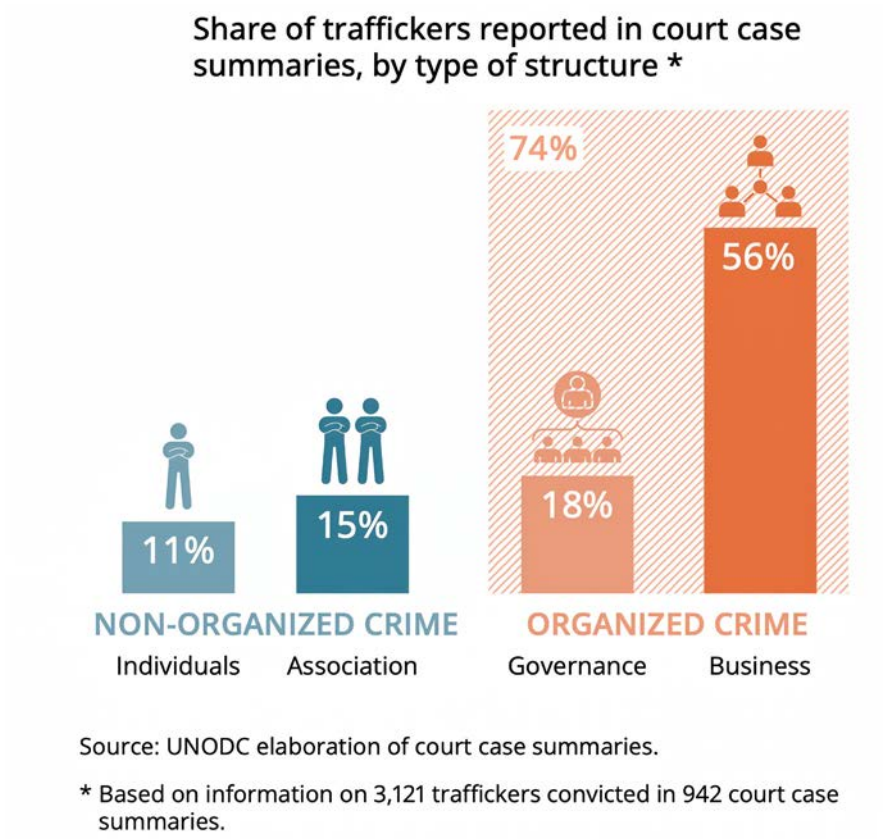
Source: https://www.unodc.org/documents/data-and-analysis/glotip/2024/GLOTIP2024_Chapter_1.pdf

17 *International Criminal Court, 2023.* https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-vladimir-vladimirovich-putin-and accessed 14 Oct. 2025

18 *Wikipedia, 2025.* https://en.wikipedia.org/wiki/Child_abductions_in_the_Russo-Ukrainian_War accessed 14 Oct. 2025

Another example comes from different geographical region, China, between 2010 and 2012, a series of suicides occurred at the facilities of Foxconn Technology Group, a major electronics manufacturer in Shenzhen, known for producing components for companies such as Apple, Sony, and other global tech giants. During this period, at least 14 workers died by suicide, with most victims jumping from the dormitory buildings on factory grounds. The majority of those affected were young migrant workers who had relocated from rural areas of China in search of employment. Working and living conditions within Foxconn factories was unacceptable to our western standards. In response to mounting public criticism and pressure from corporate clients, Foxconn implemented a number of measures aimed at preventing further tragedies. Most notably, the company installed anti-suicide nets on its buildings to physically deter further incidents.[19]

Chart No. 2



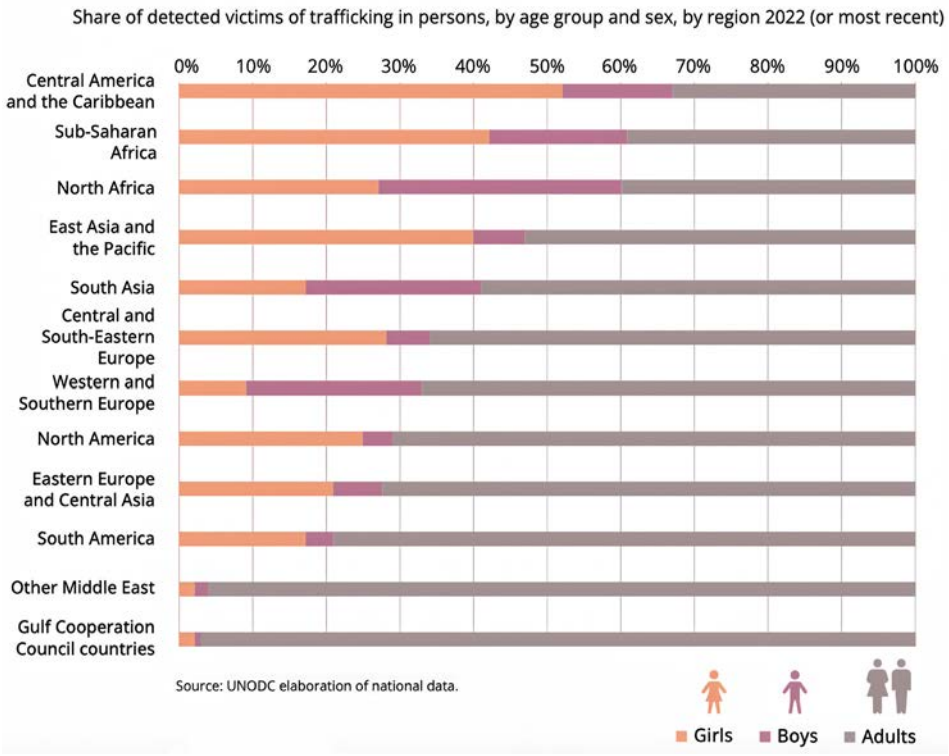
Source: https://www.unodc.org/documents/data-and-analysis/glotip/2024/GLOTIP2024_Chapter_1.pdf

19 *Industriall, 2010.* https://www.industriall-union.org/archive/imf/foxconn-electronics-workers-suicide-in-china accessed 14 Oct. 2025

Example from US, Jeffrey Epstein case, a wealthy American financier, and Ghislaine Maxwell, a British socialite, were at the centre of one of the most high-profile sex trafficking scandals of the 21st century. Epstein was accused of operating an extensive sex trafficking network, targeting underage girls, many of whom were recruited under the guise of offering financial support or employment opportunities. Ghislaine Maxwell was identified as a key accomplice who helped groom and recruit victims. The abuse, which spanned decades, involved powerful individuals and took place in multiple locations, including Epstein's private island, New York mansion, and Florida residence. Despite early legal troubles in the mid-2000s, Epstein managed to avoid serious consequences through a controversial plea deal. However, renewed investigations led to his arrest in 2019. He died shortly after in jail under suspicious circumstances, officially ruled as suicide. Maxwell was later arrested in 2020 and stood trial in 2021. She was found guilty on several counts, including sex trafficking of minors, and sentenced to 20 years in prison. The case highlighted systemic failures in addressing sexual abuse, the influence of wealth and power, and the global reach of trafficking networks. It also reignited public discourse on justice for survivors and accountability for elite offenders.[20] As we can see from the above examples modern slavery has many faces, but its common, unchanged denominator remains the same: exploitation, often through deception, coercion, or the abuse of vulnerability and can be perpetrated by individuals or state actors.

20 Bill Chappell, *Jeffrey Epstein files: Tracing the legal cases that led to sex-trafficking charges, NPR, 2025,* https://www.npr.org/2025/07/25/nx-s1-5478620/jeffrey-epstein-crimes-timeline-legal-case accessed 14 Oct. 2025

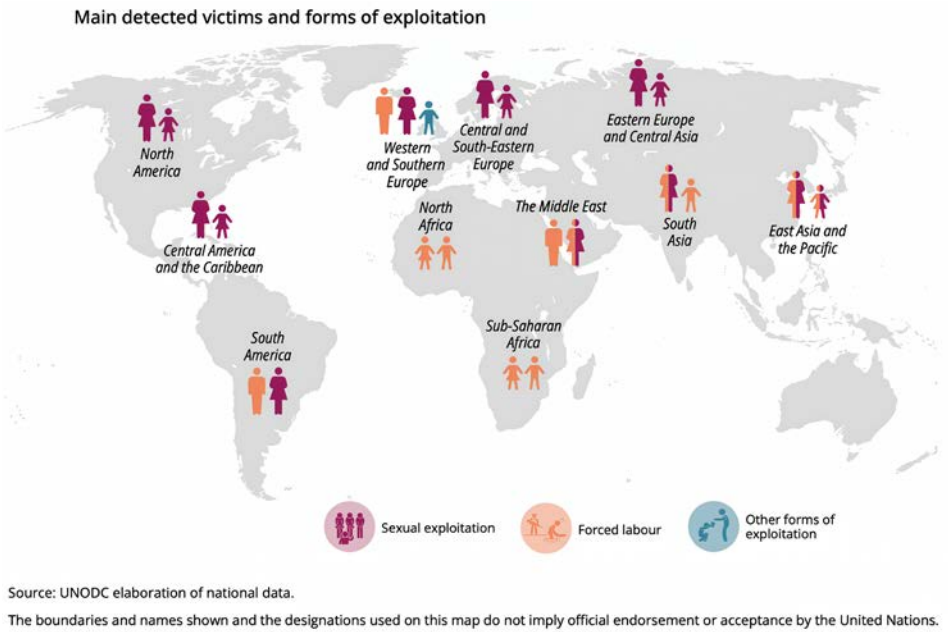
Chart No. 3



Source: https://www.unodc.org/documents/data-and-analysis/glotip/2024/GLOTIP2024_Chapter_1.pdf

Monitoring organizations have reported an increase in sexual exploitation and forced labour in both war-affected regions and beyond. Areas such as Syria, Yemen, and those impacted by the conflict between Israel and Hamas serve simultaneously as sources and destinations for human trafficking. While significant research is still needed to fully assess the scale of the problem, ongoing military actions and political instability hinder reliable academic inquiry.

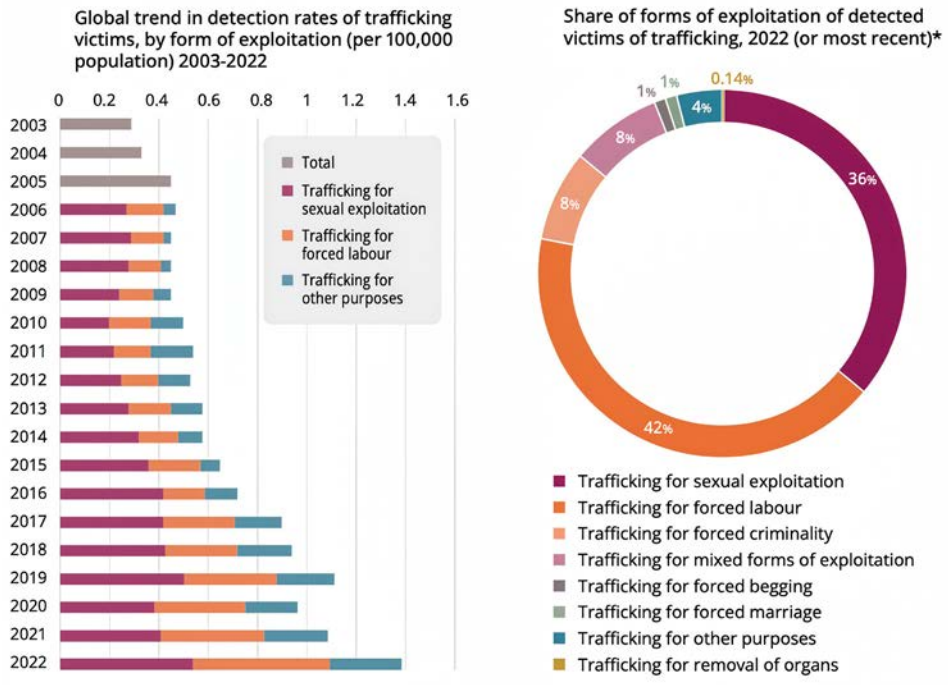
Chart No. 4



Source: https://www.unodc.org/documents/data-and-analysis/glotip/2024/GLOTIP2024_Chapter_1.pdf

Armed conflicts, migration, and fragile governance further fuel this phenomenon, manifesting in the sexual exploitation of women and children as well as the forced labour of migrants. South America, in countries such as Brazil, Colombia and Peru, human trafficking takes the form of sexual exploitation, forced labour in agriculture, and drug trafficking involving children and adolescents. Mexico and US fighting a war with cartels known for brutal tactics and diversified criminal operations such as Jalisco New Generation Cartel (CJNG), Los Zetas, Sinaloa, Juárez or Gulf Cartel, combating human trafficking problems alongside with drug trafficking. In times of chaos, criminals can recruit victims more easily, border controls are weakened and state apparatus is dysfunctional.

Chart No. 5



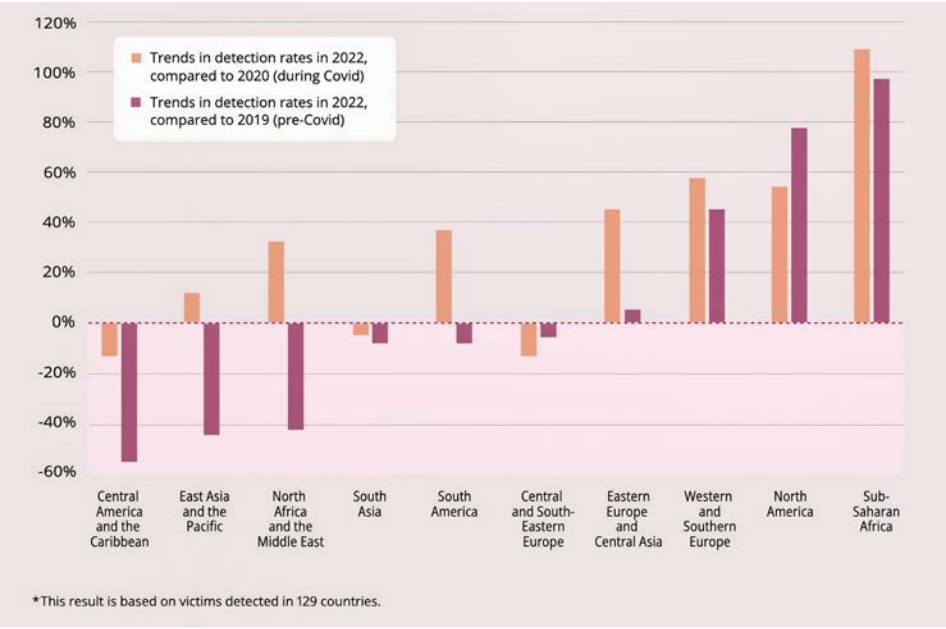
Source: https://www.unodc.org/documents/data-and-analysis/glotip/2024/GLOTIP2024_Chapter_1.pdf

Migrations crises driven by persecution, poverty, or climate change increase the number of people at risk of exploitation. Migrants often cross borders illegally, which makes it more difficult for them to obtain legal protection. It is essential to draw a distinction between human trafficking and migrant smuggling. Human trafficking is characterized by the exploitation of individuals, in contrast, migrant smuggling involves a consensual arrangement between a migrant and a smuggler to facilitate unauthorized border crossing. While trafficking constitutes a grave violation of fundamental human rights, smuggling primarily represents an infringement of national immigration and border control regulations. Conversely, smuggling may form part of a human trafficking operation when individuals are transported without their genuine consent and the smuggler engages in the exploitation of their person. Poverty and lack of prospects, combined with limited access to education and employment, leads many people to undertake risky journeys and accept dubious job offers, which often result in forced exploitation.

Summary conclusion

The Trafficking in Persons (TIP) Report, published annually since 2001 by the U.S. State Department's Office to monitor and combat trafficking, it evaluates and ranks governments according to their efforts to address human trafficking, using criteria from the Victims of Trafficking and Violence Protection Act of 2000.[21] The ranking system has four main categories: Tier 1 – Governments fully comply with TVPA minimum standards. Tier 2 – Governments do not fully comply but are making significant efforts. Tier 2 Watchlist – Same as Tier 2, but with significant victim numbers, lack of progress, or reliance on future commitments. Tier 3 – Governments neither comply nor make significant efforts. According to the UNODC, human trafficking affects millions of people worldwide, but documented cases represent only a fraction of the real scope due to the hidden nature of the crime. For instance, between 2020- 2023, 202,478 trafficking victims were detected across 156 countries, yet the actual numbers remain much higher.[22]

Chart No. 6

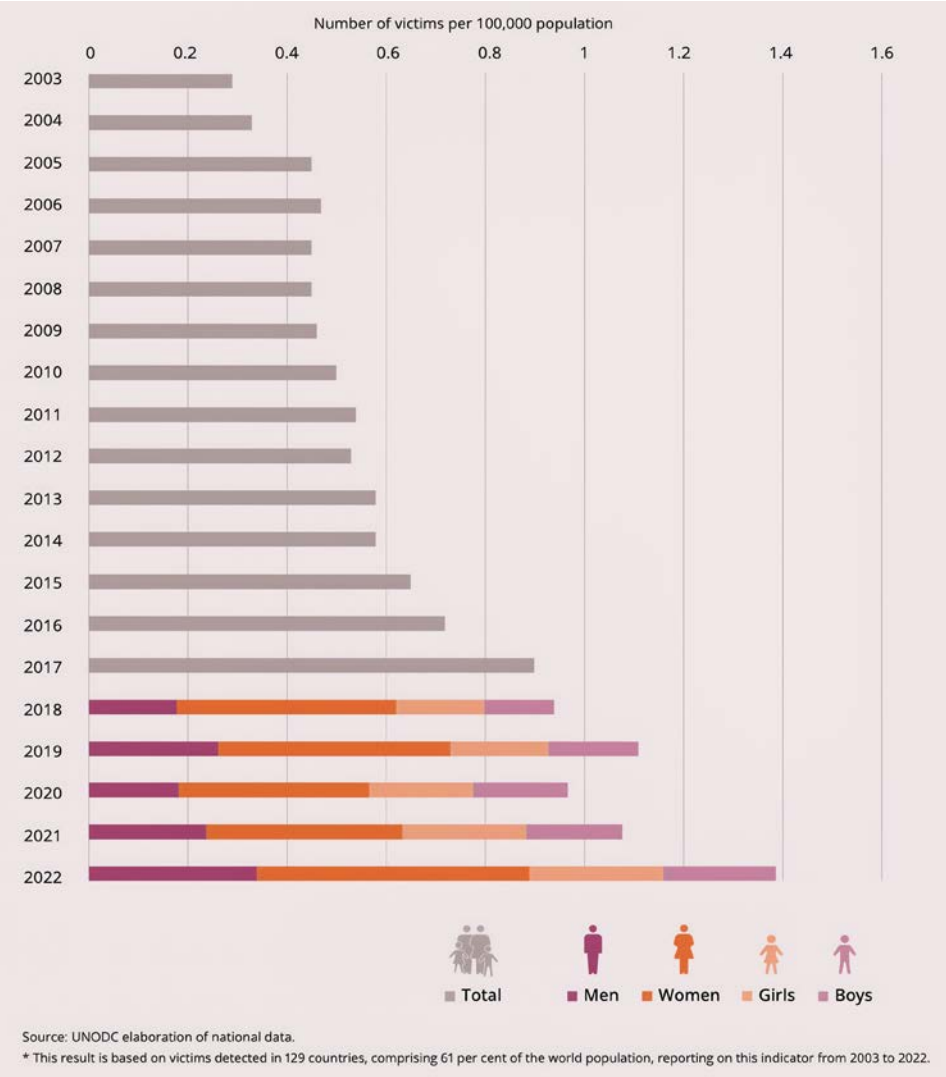


Source: https://www.unodc.org/documents/data-and-analysis/glotip/2024/GLOTIP2024_BOOK.pdf

21 *Victims of Trafficking and Violence Protection Act*, 2000. *https://www.congress.gov/106/plaws/publ386/PLAW-106publ386.htm* accessed 14 Oct. 2025

22 Acrath, *Global Report on Trafficking in Persons, 2024*, https://acrath.org.au/2024-global-report-on-trafficking-in-persons accessed 14 Oct. 2025

Chart No. 7



Source: https://www.unodc.org/documents/data-and-analysis/glotip/2024/GLOTIP2024_BOOK.pdf

The Walk Free report indicates that around 50 million people live in conditions of modern slavery worldwide.[23] In 2024, Europol emphasized that human trafficking is the third-largest source of income for organized criminal groups in Europe.[24] Countries in Central and Eastern Europe, Southern Europe, and those serving as

23 Walk Free Foundation, *Global Slavery Index, 2023*. https://www.globalslaveryindex.org/ accessed 14 Oct. 2025

24 Europol, *EU Serious and Organised Crime Threat Assessment,2024.* https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf accessed 14 Oct. 2025

transit points are particularly at risk. Globally, it is the most profitable source of income for organized criminal groups, second only to the counterfeiting of luxury goods, the counterfeiting of pharmaceuticals, and drug smuggling. The fight against human trafficking is based on multi-level actions. Many countries have adopted national strategies and laws aimed at identifying and protecting victims, as well as prosecuting perpetrators. Educational programs and training for law enforcement officers are being implemented. The UN, the International Labour Organization (ILO), the UNODC, and other agencies coordinate activities, collect data, and promote international cooperation. NGOs often work to assist victims by providing shelter, psychological and legal support. They also organize awareness campaigns and training sessions. Despite the involvement of many stakeholders, combating human trafficking faces numerous challenges. Victims often do not report to the authorities due to fear, stigma, or lack of trust. There is a shortage of effective identification tools, which makes providing assistance more difficult. After being freed, victims often do not receive adequate support, increasing the risk of returning to exploitative situations. Criminals use advanced methods of concealment, and weak legal frameworks as well as corruption hinder effective prosecution. The contemporary face of human trafficking is extremely complex, reflecting changing social, political, and technological realities. The scale of the phenomenon is immense, and its forms are diverse. Despite existing countermeasures, it is necessary to further intensify efforts, especially in the areas of victim identification, public education, data accessibility and international cooperation and prosecution. Only a comprehensive approach will make it possible to effectively curb this violation of human rights.

Bibliography

An Act for the Abolition of the Slave Trade (47 Geo. III Sess. 1 c. 36).

Acrath, *Global Report on Trafficking in Persons*, 2024, https://acrath.org.au/2024-global-report-on-trafficking-in-persons

Bales K., *Disposable people: New slavery in the global economy*, University of California Press, 2004.

Directive 2011/36/EU of the European Parliament and of the Council, 5 April 2011.

Dutch Criminal Code. Article 273f.

Eltis D., *The rise of African slavery in the Americas*, Cambridge University Press, 2000.

European Commission, *Newly released data show increase in trafficking in human beings,* 28 February 2024. https://home-affairs.ec.europa.eu/news/newly-released-data-show-increase-trafficking-human-beings-2024-02-28_en

Europol, *EU serious and organised crime threat assessment, SOCTA*, 2024, https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

French Penal Code. Articles 225-4-1, 225-4-2, 225-4-3.

German Criminal Code (Strafgesetzbuch, StGB). Section 232.

IndustriALL Global Union, *Foxconn electronics workers' suicide in China*, 2010. https://www.industriall-union.org/archive/imf/foxconn-electronics-workers-suicide-in-china

International Criminal Court, *Situation in Ukraine, ICC judges issue arrest warrants against Vladimir Vladimirovich Putin and others*, 2023. https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-vladimir-vladimirovich-putin-and

Mariposa Foundation, *Every 30 seconds another person becomes a victim of human trafficking,* 2019. https://www.mariposacenter.org/blog/every-30-seconds-another-person-becomes-a--victim-of-human-trafficking/

National Institute of Justice, *Gaps in reporting human trafficking incidents result in significant undercounting, 2020.* https://nij.ojp.gov/topics/articles/gaps-reporting-human-trafficking-incidents-result-significant-undercounting

National Public Radio, *Timeline: The crimes and legal cases of Jeffrey Epstein, 2025.* https://www.npr.org/2025/07/25/nx-s1-5478620/jeffrey-epstein-crimes-timeline-legal-case

Polish Penal Code. Article 189a-1.

Thirteenth Amendment to the United States Constitution.

Trafficking Victims Protection Act,TVPA, 2000, Public Law 106-386, 114 Stat. 1464. https://www.congress.gov/106/plaws/publ386/PLAW-106publ386.htm

United Nations, *Palermo Protocol, 2000.*

United States Code. (n.d.). 18 U.S. Code §§ 1589, 1584, 1590.

Walk Free Foundation, *Global slavery index*, 2023. https://www.globalslaveryindex.org/

Wikipedia, *Child abductions in the Russo-Ukrainian War*, 2025 https://en.wikipedia.org/wiki/Child_abductions_in_the_Russo-Ukrainian_War

Worldometer, *GDP by country*, 2023. https://www.worldometers.info/gdp/gdp-by-country/

About the Author

Lukasz Mileszko (MPhil), Doctoral Candidate in Security Sciences Studies, WSB Academy. Holds a Bachelor's degree in National Security and Counterterrorism Studies from the University of Security (WSB), Poznan, and a Master's degree in International Peace Studies from Trinity College, Dublin. Security consultant.

Bartosz Janiszewski M.Sc.
WSB University in Dąbrowa Górnicza
janis.wopr@gmail.com
ORCID: 0009-0007-0789-2688

DOI: 10.26410/SF_2/25/6

PERSONAL SAFETY OF CHILDREN IN THE CONTEXT OF FULL-FACE SNORKEL MASK USE: RISK ANALYSIS OF HYPERCAPNIA AND HYPOXAEMIA

Abstract

The article presents the risks associated with the use of full-face snorkeling masks. In children. Based on scientific research findings, the risk of hypercapnia and hypoxemia It is discussed, this may result from rebreathing air with a high concentration of CO_2. Particular attention is given to the increased risk in children due to their smaller tidal volume and a higher ratio of dead space to lung volume. The lack of safety standards for this type of equipment and difficulties in its use during emergencies are also highlighted.

Keywords

snorkeling, full-face mask, hypercapnia, hypoxemia, children, safety

Introduction

Snorkeling is the younger cousin of freediving and the stepbrother of scuba diving, which has gained enormous popularity worldwide as a separate form of water recreation accessible to a broad range of people. While freediving is a sport of holding one's breath for as long as possible, snorkeling involves observing the underwater world from the water's surface with only the face submerged, protected by a specialized mask, and breathing atmospheric air through a tube that is an integral part of the mask. Unlike scuba diving, snorkeling does not require complicated and expensive equipment or specialized training[1]. Overall, diving is often described as an activity for everyone. It is not reserved for heroes of the deep sea. Physical fitness is limited to packing your equipment into a car trunk or into a boat. Once submerged, physical conditions cease to play a significant role[2]. Consequently, snorkeling may seem like an even easier sport to start exploring the underwater world and, often mistakenly, safer for beginners. The basic equipment for snorkeling includes a mask, a snorkel, and fins, making the gear much cheaper and more accessible than scuba diving with tanks. The lack of need for long courses or certification further increases the popularity of this form of underwater exploration[3].

In recent years, innovative full-face snorkeling masks have emerged on the market, enabling simultaneous breathing through both the nose and mouth while providing a wide underwater field of view. Their design quickly gained popularity, especially among amateurs and families with children[4]. However, along with the widespread use of this equipment, serious safety concerns have also arisen, particularly regarding its use by children. These issues mainly relate to the risk of carbon dioxide poisoning (hypercapnia) and hypoxia (oxygen deficiency), which can result from faulty airflow and the re-breathing of exhaled CO_2 inside the mask.

This article aims to present a catalog of hazards associated with the use of full-face snorkeling masks in children, based on scientific research findings. It will discuss specific risk factors resulting from the particular physiological characteristics of children, which make them more vulnerable to the effects of hypercapnia and hypoxia during the use of this type of equipment.

Methodology

The research problem of this study arises from the lack of sufficient scientific data and technical standards concerning the safety of full-face snorkeling masks for children. There is a justified concern that the design of these masks, characterized by

1 D. Rebikoff, *Free Diving*, wyd. Sidgwick & Jackson, Londyn 1955, p. 6

2 P. Tailliez, F. Dumas, C. Jacques-Yves, *The Complete Manual of Free Diving*, wyd. G. P. Putnam's Sons, Nowy Jork 1957, p. 11

3 S. Hong, H. Rahn, „The Diving Women of Korea and Japan", *Scientific American,* 1967;216(5):34–43. [PubMed], [access: 19.07.2025].

4 H. B. Newton, „Neurologic complications of scuba diving", *American Family Physician,* 2001 Jun 1;63(11):2211-8. PMID: 11417773 [access: 08.08.2025].

a significant dead space volume, may lead to an increased risk of hypercapnia (carbon dioxide buildup) and hypoxemia (oxygen deficiency), especially under physical exertion conditions. This issue is further compounded by the fact that most available studies pertain to adults, and conclusions regarding children are mainly based on extrapolation, without extensive empirical research.

In this context, the main research question has been formulated: how does the use of full-face snorkeling masks by children affect the safety of their health and life, with particular emphasis on the risk of hypercapnia and hypoxemia?

Specific questions include the following issues:

1. What are the potential mechanisms leading to CO_2 accumulation in full-face snorkeling masks for children?
2. To what extent does the dead space volume in a full-face mask exceed the tidal volume of a child in different age groups?
3. What conclusions can be drawn from studies on adults regarding their application to the pediatric population?
4. What prophylactic measures and recommendations can be formulated to reduce the risks for children using this type of equipment?

The main objective of this study is to assess the hazards resulting from the use of full-face snorkeling masks by children in the context of their health and safety. Specific goals include:

- Analyzing the construction of full-face snorkeling masks in terms of dead space volume and its impact on gas exchange in children,
- Reviewing scientific research related to hypercapnia and hypoxemia associated with the use of full-face masks,
- Identifying gaps in current knowledge and the absence of safety standards for full-face masks designed for children,
- Developing recommendations for parents, guardians, and manufacturers regarding the safe use of snorkeling equipment by the youngest users.

This study is of a review nature. Particular emphasis was placed on assessing the risk of hypercapnia (carbon dioxide poisoning) and hypoxemia (oxygen deprivation), resulting from rebreathing air with elevated CO_2 content. The analysis was conducted based on available scientific publications, experimental research, and technical documentation provided by snorkeling equipment manufacturers in user manuals.

The review included studies available in the PubMed, Scopus, and Google Scholar databases, published between 2010 and 2024, with particular attention to peer-reviewed articles. The selection of publications was based on the presence of keywords such as: full-face snorkel mask, CO_2 retention, hypoxemia, hypercapnia, snorkeling safety, children, dead space, tidal volume.

Physiological data regarding the tidal volume of children aged 3 to 10 years were also incorporated, referencing the dead space volume of typical full-face masks presented in available studies. To assess the risk, a comparison was made between the

ratio of mask volume to the tidal volume (TV), with exceeding 100% being considered potentially dangerous.

This review does not include original research or laboratory measurements; its character is conceptual. Due to the limited availability of studies on children, some conclusions are based on theoretical modeling and extrapolation of results from research on adults. The only actual study conducted in this area was the determination of the volume of full-face snorkeling masks through water immersion measurements to assess dead space volume.

Analysis of hazards resulting from the use of full-face masks by children

When considering the hazards that may cause changes in the normal values of vital parameters in children, one must start by defining the normal ranges of these parameters. According to the Guidelines of the European Resuscitation Council, the tidal volume is a constant value and does not change throughout a person's life. It is assumed that the normal tidal volume is in the range of 6-8 ml/kg of body weight[5]. Knowing the child's weight at various ages makes it easy to precisely determine the volumes at which a young person should breathe. Estimative, medicine uses the following formula to determine the body weight of a child up to 10 years old:

$$\text{body weight (kg)} = 2 \times (\text{age of the child} + 4)$$

Table 1. Recommended Body Weight Based on Child's Age

Age of the child (years)	Recommended Body Weight (kg)
3	14
4	16
5	18
6	20
7	22
8	24
9	26
10	28

Source: Own calculation based on the formula: body weight (kg) = 2 x (child's age + 4). Based on Pediatric Formulas[6].

5 P. Van de Voorde, N. M. Turner, J. Djakow, „10 Resuscitation Procedures in Children" [in:] *Resuscitation Guidelines 2021 of the European Resuscitation Council*, Perkins G. D., Polish Resuscitation Council Publishing, Kraków 2021, p. 385

6 T. Janus, J. Nelle, *Wzory pediatryczne – wersja podręczna*, https://intensywna.pl/wzory-pediatryczne-wersja-podreczna/, [access: 18.08.2025].

Considering the above, it is worth pondering whether the use of full-face masks by children does not pose a safety risk, especially since we know that tidal volume is closely related to body mass.

In 2003, research by Janneke Grundemann, Xavier C.E. Vrijdag, Nicole Y.E. Wong, Nicholas Gant, Simon J. Mitchell, and Hanna van Waart was published in the diving magazine Diving and Hyperbaric Medicine[7].

The authors assumed that airflow as a breathing mixture in a full-face snorkel mask (FFSM) used for snorkeling should be unidirectional to prevent re-breathing the same air.

Their study evaluated the impact of re-breathing air from a full-face mask compared to a traditional mask and snorkel setup. The research involved comparing full-face snorkeling masks (Subea Easybreath and QingSong 180°) with a conventional mask plus snorkel (Beuchat Spy) in 20 adult participants under resting conditions and during light to moderate physical activity. They measured oxygen saturation levels (SpO_2) and end-tidal carbon dioxide pressure ($etCO_2$). The results indicated that users of full-face masks more frequently experienced hypercapnia (elevated CO_2 levels) and hypoxemia (reduced oxygen levels) compared to those using traditional masks. In some cases, testing was halted due to exceeding safe CO_2 thresholds (>7.0 kPa) or oxygen saturation dropping below 85%.

Eleven years later, in 2022, a study by Harald Walach, Rainer Weikl, Jan Prentice, and others was published in Environmental Research[8]. The authors assessed the ventilation and oxygenation capacity of children, assuming that children have significantly lower adaptive abilities due to the anatomy of their respiratory system. The experiment measured inhaled carbon dioxide levels in healthy children wearing surgical masks and FFP2 masks while seated for approximately 18 minutes. a significant increase in CO_2 levels in inhaled air was observed, exceeding accepted safety standards. This study highlights that children are more susceptible to CO_2 accumulation due to their smaller tidal volumes and a higher ratio of dead space to lung volume.

What, then, is the implication of the study on children using FFP2 protective masks for their safety when using full-face snorkeling masks?

Research conducted on children using protective masks showed that, due to their respiratory anatomy, children have considerably lower adaptive capacity to tolerate elevated CO_2 levels and decreased blood oxygen. It is important to note that a protective mask that is not fully airtight, by not fitting completely to the child's face, delivered significantly higher amounts of oxygen during the study than a fully fitting

7 J. Grundemann, X. C. Vrijdag, N. Y. Wong, N. Gant, S. J. Mitchell & H. van Waart, (2023). „Full-face snorkel masks increase the incidence of hypoxaemia and hypercapnia during simulated snorkelling compared to conventional snorkels", *Diving and hyperbaric medicine*, 53(4), 313–320. https://doi.org/10.28920/dhm53.4.313-320 [access: 19.07.2025].

8 H. Walach, H. Traindl, J. Prentice, R. Weikl, A. Diemer, A. Kappes & S. Hockertz, (2022). „Carbon dioxide rises beyond acceptable safety levels in children under nose and mouth covering: Results of an experimental measurement study in healthy children", *Environmental research*, 212 (Pt D), 113564. https://doi.org/10.1016/j.envres.2022.113564 [access: 19.07.2025].

full-face mask. Therefore, both studies indicate potential risks associated with the use of full-face snorkeling masks, especially in children.

Another aspect to consider is the tidal volume values in children. Based on calculations by the European Resuscitation Council and the relationship between tidal volume and body mass[9], their respiratory capacities should be compared with the technical limitations of full-face snorkeling masks.

Table 2. Respiratory volumes depend on the child's age and weight

Age in years	Body Weight	Tidal volume (TV)		Average tidal volume (TV)
		for 6ml/kg BW	for 8ml/kg BW	
3	14	84	112	98
4	16	96	128	112
5	18	108	144	126
6	20	120	160	140
7	22	132	176	154
8	24	144	192	168
9	26	156	208	182
10	28	168	224	196

Source: author's own compilation. Based on Resuscitation Procedures in Children[10].

The table presents respiratory values for 6 ml/kg of body mass, 8 ml/kg of body mass, and the average tidal volume for a specific age and child's weight. The data indicate that as the child gets older and the weight increases, the tidal volume also increases.

Among commercially available full-face masks on the market, depending on the manufacturer and model, their capacity ranges from 150 to 250 ml. Without detailed calculations, it is evident that these capacities significantly exceed the child's tidal volume. This brings us to the concept of dead space. Dead space refers to a specific portion of gas, in this case, air, that for various reasons does not participate in gas exchange. This phenomenon naturally occurs during breathing when exhalation does not empty the lungs of air. The remaining volume of air in the lungs is called residual volume. Due to its natural occurrence in the breathing mechanism, the body can function properly with this residual air in the lungs. However, the situation is different when considering the residual air trapped in the space within a full-face mask.

9 P. Van de Voorde, N. M. Turner, J. Djakow, „10 Resuscitation Procedures in Children…", op. cit., p. 385
10 Id.

The danger of this phenomenon lies in the fact that this gas does not disappear from inside the mask in any way. It remains within the mask's structural space between the face and the mask shell. If calculations of the mask's volume relative to the child's ventilatory capacity show that the child is unable to fully exchange the air they breathe for fresh air, this results in rebreathing the same air they have already exhaled.

Table 3. Ratio of mask face gas volume to children's volume in different age groups

Age	NTM	TV		Average TV	The ratio of the mask volume percentage to the child's average breath volume		Average percentage ratio of full-face mask volume to the child's average breath
		For 6 ml/kg NTM	For 8 ml/kg NTM		For mask 150 ml	For mask 250 ml	
3	14	84	112	98	153%	225%	204%
4	16	96	128	112	134%	223%	179%
5	18	108	144	126	119%	198%	159%
6	20	120	160	140	107%	179%	143%
7	22	132	176	154	97%	162%	130%
8	24	144	192	168	89%	149%	119%
9	26	156	208	182	82%	137%	110%
10	28	168	224	196	77%	128%	102%

NTM – nominal Total Mass
TV – Tidal volume – volume of breath
Source: author's own study. Based on measurements of full-face mask capacities.

From the above table, it can be inferred how much larger the gas volume of the mask is compared to the tidal volume of a child in various age groups. Therefore, it must be assumed that a single exhalation by the child through the snorkel, which is an integral part of the full-face mask, exchanges only a part of the air inside the mask. But what part? The answer depends: it varies depending on the individual predispositions of the child, lifestyle, diet, health conditions, level of training, etc. However, it is important to note that, regardless of these factors, this is certainly not the full volume of the mask. Consequently, some air remains inside the mask, which does not participate in gas exchange, leading to the accumulation of CO_2 within the mask space.

In children aged 3 to 10 years, a full-face snorkel mask can have such a large capacity that it exceeds their single breath volume. In practice, this means that the child is largely breathing in air that has already been used, resulting in limited gas exchange. As a consequence, CO_2 may accumulate in the body, leading to hypercapnia, as well as hypoxia, which is a deficiency of oxygen. These gas exchange disturbances carry risks such as dizziness, loss of consciousness, and, in extreme cases, drowning.

Summary

Research has shown that the design of full-face snorkeling masks, which cover both the mouth and nose simultaneously, promotes the phenomenon known as rebreathing–re-inhaling exhaled air from the previous breathing cycle. This exhaled air, lingering in the dead space of the mask, is characterized by an elevated concentration of carbon dioxide (CO_2) and a reduced oxygen (O_2) content compared to atmospheric air. As a result, without proper venting of gases during exhalation and delivery of fresh air during inhalation, there is a gradual increase in CO_2 levels in the user's body (hypercapnia).

In one experimental study simulating snorkeling conditions, it was found that using full-face masks can cause both hypercapnia and hypoxia (low blood oxygen levels). This phenomenon was particularly pronounced during physical exertion, even at light or moderate intensity. Under such conditions, the body's metabolic demand for oxygen increases, while the rate of CO_2 production accelerates. If the mask's construction does not ensure effective ventilation and minimize dead space volume, CO_2 accumulation can occur faster than at rest, leading to symptoms such as headache, dizziness, concentration difficulties, increased heart rate, and in extreme cases, loss of consciousness, known as hypoxic blackout[11].

It is especially important to note that most existing studies have been conducted on adults, whose respiratory systems have greater capacity and better ability to compensate for gas exchange changes than children's. For younger users, due to smaller tidal volume and a higher ratio of dead space in the mask relative to lung capacity, the risk of rapid increases in CO_2 and decreases in oxygen levels is even more significant, even after short use.

Children, unlike adults, have a significantly smaller tidal volume, dependent on body mass and age. This means that in full-face snorkeling masks, the dead space (the volume of trapped air within the mask that is not effectively exchanged during each breathing cycle) constitutes a much larger proportion of a child's total lung capacity than in adults. Practically, this results in each inhalation drawing in some of the previously exhaled air, which is already enriched with CO_2 and contains less O_2. This phenomenon leads to a gradual increase in CO_2 levels (hypercapnia) and a decrease in blood oxygen (hypoxemia). The rate of these changes is faster in children due to their smaller lung volume and limited respiratory and circulatory compensatory mechanisms. Additionally, children's higher resting metabolic rate increases their oxygen requirements and CO_2 production. Coupled with less efficient mask ventilation, the risk of gas imbalance disturbances can occur after only a short period of use, even with minimal physical effort[12].

---

11 R. M. Bart, H. Lau, „Shallow Water Blackout", 2023 Jan 30. [in:] *„StatPearls. Treasure Island"* (FL): StatPearls Publishing; 2025 Jan. PMID: 32119507. [access: 02.08.2025].

12 E. Williams, T. Dassios, P. Dixon, A., „Greenough, Physiological dead space and alveolar ventilation in ventilated infants", *Pediatric Research,* 2022 Jan;91(1):218-222. doi: 10.1038/s41390-021-01388-8. Epub 2021 Feb 18. Erratum in: *Pediatric Research,* 2022 Jan;91(1):265. doi: 10.1038/s41390-021-01676-3., [access: 03.08.2025].

Consequently, in activities like playing in shallow water or slow surface swimming, a child using a full-face mask may experience a progressive and initially unnoticed deterioration in physiological state. Symptoms such as headache, drowsiness, disorientation, rapid breathing, or loss of consciousness can appear suddenly, posing an immediate drowning hazard. This issue is particularly critical if there is no strict supervision by an adult or if the mask is difficult to remove quickly in case of respiratory problems. Currently, there are no unified, precisely defined safety standards for full-face snorkeling masks at national or international levels. Unlike many other types of water sports equipment, which are certified according to clear standards (e.g., ISO, EN, or sports federation guidelines), these masks are not subject to a consistent regulatory system covering design parameters, materials, dead space volume, or ventilation efficiency.

This practical lack of regulation leads to significant variability in design and manufacturing quality, resulting in notable differences in performance and safety features across products from different brands and even among models from the same manufacturer. Some masks may feature well-designed breathing channels that minimize re-inhalation of CO_2, while others–due to simplified construction or cost-cutting–may not provide adequate gas exchange. The absence of mandatory independent laboratory testing means that consumers–especially parents purchasing masks for children–often rely solely on marketing, online reviews, or price, without a reliable assessment of safety. As a result, the market offers both relatively safe models and potentially dangerous designs, which, particularly for children with limited respiratory capacity, can lead to serious health consequences.

The lack of standardization and certification poses significant challenges for user safety and restricts effective communication about risks, as well as the implementation of uniform requirements for design, testing, and marking of this equipment. Due to their full-face design and straps that secure behind the head, these masks can be considerably more difficult and time-consuming to remove quickly in emergencies compared to traditional mask and snorkel sets. In critical situations–such as flooding of the mask, sudden unconsciousness, laryngospasm, panic attack, or breathing difficulties caused by CO_2 buildup–rapid removal of the mask from the face becomes crucial for safety.

For adults, and even more so for children, this process can be complicated if straps are too tight or twisted, or if wet hands, cold water, or limited visibility hinder manipulation of buckles or flexible materials. Every additional second needed to remove the mask in an emergency increases the risk of unconsciousness and, ultimately, drowning.

Children are especially vulnerable for several reasons: they have less manual strength, poorer panic control, and limited experience in handling sudden aquatic situations. Furthermore, for very young users, removing the mask may require adult assistance, which may not be feasible quickly in real conditions (e.g., when in water some distance from the shore).

From a rescue safety perspective, the longer it takes to remove a full-face mask in a critical situation, the greater the risk, and this factor should be carefully considered when selecting snorkeling equipment, especially for children and inexperienced users.

Full-face snorkeling masks should not be used by children under 7 years old, and in many cases, it is advisable to avoid them altogether until about age 10. This is because younger children have much smaller lung volumes and reduced respiratory compensatory capacity, and the large dead space typical of these masks significantly increases the risk of CO_2 accumulation, hypercapnia, or hypoxia[13]. Exceptions may include designs specifically developed for children, with dead space reduced to safe levels and subjected to independent, certified safety testing by qualified institutions.

However, in practice, such specialized equipment is rarely available on the market, and manufacturers' claims are often not supported by thorough testing. Therefore, for the youngest users, traditional mask and snorkel sets are recommended. This classic gear allows better control over breathing, facilitates quick and intuitive removal in emergencies, and minimizes the risk of uncontrolled CO_2 buildup. Additionally, a traditional snorkel enables easier clearing of water from the airway, which is particularly important for children still learning safe water environment navigation.

Regardless of the type of equipment chosen and the child's swimming skills, the fundamental safety rule should be constant, direct supervision by an adult who can swim and respond in emergencies. The presence of a responsible guardian or instructor significantly reduces the risk of tragic incidents such as unconsciousness underwater or drowning.

It is also important to remember that diving–whether recreational or sport–is widely regarded as an activity with increased risk of injury or death. Proper equipment, adequate preparation, awareness of potential hazards, and cautious behavior are essential. For children, this means selecting age-appropriate gear, strictly adhering to safety rules, which should take precedence over comfort or fashion. Attention should also be paid to the child's health conditions, as chronic or temporary illnesses can permanently or temporarily exclude them from diving. Common contraindications include respiratory, cardiovascular, ear and sinus disorders, eye diseases, and neurological or psychological conditions[14].

13 Trapani, L., Poropat, F., Cattaruzzi, E., Barbi, E., Zanchi, C., „Full-Face Snorkeling Masks Carry a Risk of Hypercapnia and Drowning in Younger Children: a Case Series", *Children* 2025, 12, 1148. https://doi.org/10.3390/children12091148

14 J. Krzyżak, K. Korzeniewski, *Medycyna dla nurkujących*, wyd. 4fotn, Poznań 2022, p. 14

Bibliography

Grundemann, J., Vrijdag, X. C., Wong, N. Y., Gant, N., Mitchell, S. J., & van Waart, H. (2023). „Full-face snorkel masks increase the incidence of hypoxaemia and hypercapnia during simulated snorkelling compared to conventional snorkels", *Diving and hyperbaric medicine*, 53(4), 313–320. https://doi.org/10.28920/dhm53.4.313-320, [access: 19.07.2025].

Hong S., Rahn H. „The Diving Women of Korea and Japan", *Scientific American*, 1967;216(5):34–43, PubMed, [access: 19.07.2025].

Janus T., Nelle J., *Wzory pediatryczne – wersja podręczna,* https://intensywna.pl/wzory-pediatryczne-wersja-podreczna/, [access: 18.08.2025].

Krzyżak J., Korzeniewski K., *Medycyna dla nurkujących*, wyd. 4font, Poznań 2020.

Newton H. B., „Neurologic complications of scuba diving", *American Family Physician,* 2001 Jun 1;63(11):2211-8. PMID: 11417773. [access: 08.08.2025].

Rebikoff D., *Free Diving*, wyd. Sidgwick & Jackson, Londyn 1955.

Tailliez P., Dumas F., Jacques-Yves C., *The Complete Manual of Free Diving*, wyd. G. P. Putnam's Sons, Nowy Jork 1957.

Trapani, L., Poropat, F., Cattaruzzi, E., Barbi, E., Zanchi, C., „Full-Face Snorkeling Masks Carry a Risk of Hypercapnia and Drowning in Younger Children: a Case Series", *Children* 2025, 12, 1148. https://doi.org/10.3390/children12091148 [access: 12.11.2025].

Walach, H., Traindl, H., Prentice, J., Weikl, R., Diemer, A., Kappes, A., & Hockertz, S. (2022). „Carbon dioxide rises beyond acceptable safety levels in children under nose and mouth covering: Results of an experimental measurement study in healthy children", *Environmental research*, 212(Pt D), 113564. https://doi.org/10.1016/j.envres.2022.113564, [access: 19.07.2025].

Williams E, Dassios T, Dixon P, Greenough A. „Physiological dead space and alveolar ventilation in ventilated infants", *Pediatric Research*, 2022 Jan;91(1):218-222, https://doi.org/10.1038/s41390-021-01388-8, Epub 2021 Feb 18. Erratum in: *Pediatric Research,* 2022 Jan;91(1):265, https://doi.org/10.1038/s41390-021-01388-8, [access: 03.08.2025].

Van de Voorde P., Turner N.M., Djakow J., „10 Zabiegi Resuscytacyjne u dzieci" [in:] *Wytyczne resuscytacji 2021 Europejskiej Rady Resuscytacji*, Perkins G. D., wyd. Polska Rada Resuscytacji, Kraków 2021.

Bart RM, Lau H. „Shallow Water Blackout", 2023 Jan 30. [in:] *StatPearls. Treasure Island* (FL): StatPearls Publishing; 2025 Jan. PMID: 32119507 [access: 02.08.2025]

About the Author

A practicing paramedic in the Emergency Department, WOPR Instructor No. 1202, powerboat helmsman, scuba diver and freediver. With over 20 years of experience in water rescue, he currently pursues a PhD in security sciences. a passionate advocate for public safety, human safety, and health protection–especially in extreme, high-risk situations that fall far outside everyday life. In short: a full-time safety freak.

mgr inż. Dawid Kądzioła
University of Agriculture, Faculty of Production and Power Engineering,
Department of Machinery Operation, Ergonomics and Production Processes
e-mail: dawid.kadziola@icloud.com
ORCID: 0009-0006-4464-4803

DOI: 10.26410/SF_2/25/7

CYBERSECURITY AS A KEY ELEMENT OF NATIONAL SECURITY: AN ANALYSIS OF THREATS AND DEFENSE STRATEGIES IN THE 21st CENTURY

Abstract

The aim of this article is to analyze the key role of cybersecurity in ensuring national security in the 21st century. First, the theoretical foundations of cybersecurity and the current legal framework are presented, with particular emphasis on the Polish national cybersecurity system and EU regulations, such as the NIS and NIS 2 directives. Next, the main cyber threats to the state are identified and discussed, including attacks on critical infrastructure, ransomware threats, disinformation activities, and organizational gaps and human error. The article provides a detailed analysis of cyber threat defense strategies, emphasizing the importance of synergy between the public and private sectors and the services responsible for security. The methodology used includes an analysis of scientific literature, legal acts, strategic documents, and reports from CERT/CSIRT teams. The conclusions of the analysis point to the need for a holistic approach to cybersecurity, integrating political, legal, technical, and educational measures, which is a prerequisite for effectively countering growing cyber threats.

Keywords

cybersecurity, national security, critical infrastructure, cyber threats, defense strategies

Introduction

In the era of widespread digitization, cybersecurity has become an integral part of national security. Critical state infrastructure, public services, and the private sector increasingly rely on ICT systems, which brings with it new types of threats. The scale of these threats is growing rapidly–for example, according to FBI data, 2020 saw a 400% increase in the number of cyberattacks[1] – and similar trends are observed in Poland, where CERT Polska recorded as many as 34% more cybersecurity incidents than in the previous year. Cyberattacks are no longer isolated incidents – they are now a daily challenge for public administration at all levels. The consequences of successful cyberattacks can be very serious. Disruption of the power grid, financial system, or transportation system threatens the stability of the state in a way comparable to traditional physical threats. The disclosure or encryption of sensitive citizen data undermines trust in public institutions and compromises the privacy of society. Cyber-attacks can also limit the state's ability to provide basic services and respond to emergencies. Cybercrime poses a threat not only to the efficient functioning of local governments, but also to the entire state and the security of its citizens[2]. For this reason, countries around the world have recognized cyberspace as a key area of their security strategy.

This article analyzes the most serious cybersecurity threats to state security in the 21st century and presents defense strategies, with particular emphasis on the Polish legal and institutional context.

Theoretical part

Cybersecurity is sometimes defined in legal terms as "the resilience of information systems against actions that violate the confidentiality, integrity, availability, and authenticity of processed data or related services," as stated in the Act of July 5, 2018, on the national cybersecurity system[3]. This definition emphasizes that the essence of cybersecurity is to ensure the continuity and trustworthiness of information and communication systems despite attempts at disruption or attacks. Cybersecurity has become an integral part of national security, as modern states cannot function without efficient IT systems supporting administration, the financial sector, energy, communications, healthcare, and other key services. a breach of cybersecurity can therefore translate into real threats to public order, the economy, and even the lives of citizens.

In response to growing threats, Poland, like other European Union countries, has developed a legal and institutional framework to protect cyberspace. The aforementioned Act on the National Cybersecurity System of 2018 implements the provisions

1 A.F. Ruggiero, T. Owosu, *Ransomware in local government: Risk factors, vulnerabilities, and exploitation during a global pandemic*, Issues in Information Systems 2022, No 23(4), p. 184.

2 T.T.P. Cortese, J.F.S.d. Almeida, G.Q. Batista, J.E. Storopoli, A. Liu, T. Yigitcanlar, *Understanding Sustainable Energy in the Context of Smart Cities,* a Prisma Review Energies 2022, No 15, 2382, p. 3.

3 Act on the National Cybersecurity System of 5 July 2018. (2018). *Journal of Laws of the Republic of Poland*, item 1560, as amended.

of the EU's 2016 NIS Directive (Network and Information Systems), defining the organization of the cybersecurity system at the national level. In accordance with the Act, the National Cybersecurity System (KSC) was established to ensure the uninterrupted provision of IT services and efficient incident management[4]. The system includes, among others, operators of essential services (OUK) in designated sectors, digital service providers, computer incident response teams (CSIRT) at the national and sectoral levels, as well as administrative bodies responsible for cybersecurity. According to the Act, operators of essential services are entities from sectors as important as energy, transport, banking and financial market infrastructure, healthcare, drinking water supply and digital infrastructure[5]. The Act imposes a number of obligations on these entities and selected administrative bodies, including the implementation of adequate security measures, conducting risk analyses, and reporting incidents within 24 hours of their detection to the relevant CSIRTs. Importantly, every serious or critical incident must be handled in cooperation with the relevant authorities, ensuring the exchange of information and necessary data. Such a reporting and response system aims to quickly stop the spread of attacks and limit their impact. Within the KSC, there are three main national CSIRT teams – at the Internal Security Agency (CSIRT.GOV), the Ministry of National Defense (CSIRT.MON) and the Research and Academic Computer Network (CSIRT.NASK) – which coordinate incident response in their respective areas. In addition, there are sectoral cybersecurity teams, and the relevant ministers perform coordination functions in specific sectors (e.g., energy, transport, healthcare). The entire system is supported by a central coordinator, currently the Chancellery of the Prime Minister through the Secretariat of the Government Plenipotentiary for Cybersecurity. The Polish model is therefore sectorally dispersed but with central strategic coordination – the Cybersecurity Strategy of the Republic of Poland for 2019-2024 sets out the objectives and directions of state policy in this area (replacing the previous Cybersecurity Policy Framework 2017-2022). The NIS Directive has laid the foundations for a coherent and integrated cybersecurity system in Europe, strengthening protection against growing threats in cyberspace[6]. In 2022, the EU adopted the new NIS 2 Directive, which further expands the scope of entities covered by the regulations (including medium-sized enterprises from additional sectors, election administration, space, postal services, etc.) and tightens requirements for incident reporting and risk management. NIS 2 emphasizes, among other things, increasing the responsibility of management for cybersecurity in organizations and strengthening cross-border cooperation. The implementation of this directive into Polish law will further strengthen the system and adapt it to the evolving threat landscape.

4 M. Terlecka-Maciejewska, *Cybersecurity in Polish security system*. Zeszyty Naukowe Politechniki Śląskiej, seria Organizacja i Zarządzanie 2024, No 198, pp. 561–571.

5 A. Chodakowska, S. Kańduła & J. Przybylska, *Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done*. Lex Localis – Journal of Local Self-Government, No 20(1), pp. 161–192.

6 Ibidem pp. 161-192.

In addition to legal regulations, the theoretical dimension of cybersecurity is constituted by information security management norms and standards. International standards, such as ISO/IEC 27001 or the American NIST Cybersecurity Framework, provide systematic methods for risk assessment and implementation of appropriate security measures. Research has shown that a significant proportion of Polish local government units have implemented an Information Security Management System (ISMS) – in one study, as many as 76.9% of municipalities declared that they had such a system, of which 82.2% complied with the ISO 27001 standard[7]. Standardizing security practices and having a formal policy increases resilience to attacks, although, as the audit results show, simply having documents is not enough. Effective implementation of policies in practice and raising staff awareness are key. For this reason, cybersecurity theory emphasizes a holistic approach that combines technical, organizational, and human aspects. In particular, the concept of a socio-technical system highlights that security is not just about hardware and software, but also about people–their knowledge, habits, and adherence to procedures[8]. People are often the weakest link in a system, so factors such as safety culture and user education must be taken into account in the overall security strategy.

To sum up the theoretical part, a 21st-century state must view cybersecurity as an element of national security. Building resilience requires a legal framework, institutions responsible for response, the application of standards, and continuous awareness-raising and competence-building in the field of cyber threats. Only an integrated approach, involving cooperation between multiple actors and consistency of action, can address the nature of threats emanating from cyberspace.

Risk analysis

Contemporary cyber threats to national security are diverse and constantly changing. The most important categories include attacks on critical infrastructure, ransomware, disinformation, and organizational vulnerabilities (internal errors and negligence). These threats are discussed below, along with examples of their impact on national security.

Attacks on critical infrastructure

Critical infrastructure includes systems and facilities that are essential for the functioning of the state and society, such as energy networks, water supply, communication systems, transport, financial infrastructure, and healthcare. Cyber attacks targeting critical infrastructure can cause physical disruptions to the provision of essential services. For example, the high-profile attack on Ukraine's power grid in

7 Ibidem, pp. 161-192.

8 M. van Haastrecht, B. Yigit Ozkan, M. Brinkhuis & M. Spruit, *Respite for SMEs: a Systematic Review of Socio-Technical Cybersecurity Metrics*. Applied Sciences 2021, No 11(15).

December 2015 caused a temporary power outage for approximately 225,000 customers, demonstrating the potential of a cyberattack to cause a real energy crisis. This was the first documented case of a successful disruption of an electricity grid using malware (BlackEnergy). a year later, Ukraine again experienced a cyberattack (Industroyer) on its electrical infrastructure, confirming experts' belief that cyberattacks have become a tool not only for criminal groups, but also for hostile states and terrorists. Wide-ranging incidents have also been reported in other countries: in 2021, a ransomware attack on the Colonial Pipeline fuel pipeline in the US paralyzed gasoline distribution on the east coast, forcing a state of emergency to be declared for fuel supplies in the region. These examples prove that critical infrastructure is a target for cybercriminals and hostile states, and that a successful attack can disrupt a country as severely as traditional acts of sabotage. Poland has not yet experienced a cyberattack on critical infrastructure with effects comparable to the above examples, although attempts and incidents on a smaller scale have taken place. In 2020, the local government railways in the West Pomeranian Province were the victim of an attack that briefly disrupted train control systems–an incident that was also considered a potentially dangerous precedent in the transport sector. In August 2023, the media reported on the disruption of the PKP railway network due to unauthorized transmission of "radiostop" signals, which was identified as a possible hybrid operation with a cyber component. The energy and financial sectors are constantly being tested for resilience – APT (Advanced Persistent Threat) attacks, often attributed to foreign intelligence services, attempt, for example, to penetrate the networks of power plants or banks for the purpose of long-term, difficult-to-detect espionage or sabotage. Threats to critical infrastructure are therefore very real, and their materialization could threaten national security, public order, and even the health and lives of citizens on a massive scale. The literature on the subject emphasizes that the growing number of systematic attacks on critical infrastructure is a global problem and requires effective international cooperation and the development of standards for regulating cyberspace[9].

Ransomware – digital extortin

Ransomware is malicious software that encrypts a victim's data and demands a ransom for its decryption. In recent years, ransomware has grown into one of the most serious threats to public institutions and businesses. These attacks have evolved from randomly infecting home users to deliberate "big game hunting" – targeting critical or high-value organizations such as hospitals, government agencies, universities, and large enterprises[10]. Local governments have become a particularly frequent target of

9 T. Baranovska, V. Savitskyi, M. Serbov, Y. Stoliar & Y. Krutik, *The impact of cybercrime on state and institutional security: Analysis of threats and potential protection measures.* Economic Affairs 2024, No 69 (Special Issue), pp. 33–42.

10 A. F. Ruggiero, T. D. Owusu & J. J. Staley, *Ransomware in local government: Risk factors, vulnerabilities, and exploitation during a global pandemic.* Issues in Information Systems 2022, No 23(4), pp. 183–191.

ransomware attacks because they hold valuable data and perform key functions for the community, while often having limited IT resources and outdated infrastructure, which makes them vulnerable to this type of attack. The effects of a ransomware attack on a government agency or institution can be serious: loss of access to systems and data paralyzes the provision of public services, from issuing documents to administering social benefits. In addition, the leakage or lack of control over citizens' data violates information security and trust in the authorities. Unfortunately, many of the entities attacked, lacking backups or contingency plans, succumb to pressure and pay ransoms to cybercriminals, which only fuels further attacks. For example, in the US, there have been high-profile cases of cities such as Atlanta and Baltimore, where ransomware attacks paralyzed city government operations for days. Atlanta suffered losses estimated at over $17 million in 2018 as a result of the SamSam attack, and Baltimore refused to pay the ransom in 2019, but the cost of rebuilding its systems exceeded $18 million – in the meantime, residents were unable to finalize real estate transactions or pay municipal bills, among other things.

Polish institutions are also not immune to such incidents. Ransomware attacks on local governments in Poland have occurred in recent years, as exemplified by the incident at the Marshal's Office of the Mazowieckie Province in December 2022. Files were encrypted as a result of malicious software, which was officially classified as a serious cybersecurity incident[11]. Similarly, the District Employment Office in Bartoszyce fell victim to an attack by a ransomware group called RansomHub, resulting in a potential breach of the personal data of the office's clients. Statistics show how widespread this problem has become – according to a report by Sophos, as many as 69% of local government institutions experienced a ransomware attack in 2022, which illustrates the scale of the threat[12]. Global data is also alarming – there has been a sharp increase in the number of ransomware attacks over the past few years. In 2020 alone, the frequency of such incidents increased several times worldwide, and cybercriminals developed entire models for carrying out attacks by less technically advanced criminals. Ransomware is therefore a hybrid threat – on the one hand, it is a form of criminal activity aimed at financial gain, damaging the financial interests and continuity of institutions; on the other hand, mass attacks of this type (e.g. the WannaCry[13] campaign in 2017) can destabilize the infrastructure of many countries simultaneously. Such attacks on hospitals or transmission networks can even endanger human lives (e.g., by blocking access to life-saving systems). Countering these attacks has therefore become a priority for many governments, and ransomware is considered one of the most serious threats to national security in cyberspace.

11 https://mazovia.pl/pl/bip/komunikaty/incydent-cyberbezpieczenstwa, access 28.04.2025 r.

12 Sophos. (2023). *The State of Ransomware in State and Local Government 2023. Retrieved from Sophos News* (news.sophos.com). – access 27.04.2025 r.

13 R. Fordoński, *WannaCry ransomware cyberattack as violation of international law*, Uniwersytet Warmińsko-Mazurski, Studia Prawnoustrojowe 2019, No 44, p. 47.

Disinformation and information warfare

In addition to purely technical attacks on systems, disinformation–the deliberate dissemination of false or manipulated information in the digital space, particularly on social media and online portals–is a significant strategic cybersecurity threat. Disinformation is a tool of so-called information warfare, often used by foreign states or organized groups to weaken social cohesion and undermine citizens' trust in democratic institutions. Unlike malware attacks, the aim of information attacks is not to directly damage IT infrastructure, but to "hack" into the public consciousness – creating divisions, spreading panic or influencing political decisions through mass propaganda campaigns on the Internet. An example of the effects of disinformation is its influence on electoral processes. The widely reported interference in the 2016 US presidential election involved, among other things, organized activity on social media, the creation of fake news, and targeted disinformation campaigns designed to polarize the electorate and influence the outcome of the election. Attempts at such information influence have also been observed in Poland–for example, during the 2018 local government campaign, the existence of fake accounts spreading false political content was revealed online. Another area of information attacks was the COVID-19 pandemic, when conspiracy theories and false information about vaccines and restrictions appeared en masse, weakening the state's efforts to combat the health crisis. Currently, in the context of the ongoing Russian-Ukrainian war, the services are warning of an intensification of pro-Kremlin disinformation aimed, among others, at at NATO's eastern flank–narratives undermining the sense of supporting Ukraine, scaring people with a refugee crisis, or slandering allies are meant to cause social unrest and reduce the political cohesion of the state.

The threat of disinformation lies in the fact that it is difficult to detect and neutralize by technical means. Combating it requires constant monitoring of information, cooperation with the media and online platforms, and raising awareness among recipients. Disinformation often accompanies other forms of aggression–it can be part of broader hybrid campaigns combining, for example, hacking attacks (the theft of compromising data) with its subsequent disclosure and manipulation of the narrative (so-called hack-and-leak). Organized disinformation campaigns pose a serious risk to national security, as they can lead to social chaos, riots, and even undermine a country's information sovereignty. In response, NATO and EU countries are developing counter-disinformation strategies. For example, the European Union has set up a special unit to combat disinformation (the East StratCom Task Force) and launched a rapid response system for fake news as part of the EU's security strategy. In Poland, the problem of disinformation has been recognized, among others, in strategic documents on information security, which point to the need to strengthen social resilience to manipulation.

Organizational gaps and internal factors

Last but not least, internal organizational gaps are another category of threats. These are shortcomings, oversights, and mistakes on the part of people, procedures, and organizational structures that enable or facilitate cyberattacks. As mentioned, the "human factor" is sometimes referred to as the weakest link in security[14]. Even the best technical safeguards can prove insufficient if users make simple mistakes or the institution fails to follow basic security rules. Typical internal problems include low awareness of threats and lack of employee training, inadequate security procedures (e.g., no password policy or access management), and shortages of qualified personnel and funding for cyber protection. Reports indicate that human error and negligence may cause even more incidents than deliberate attacks by external hackers. For example, in its 2019 report on cybersecurity in municipalities, the Supreme Audit Office (NIK) in Poland found that over 80% of the irregularities identified concerned the improper management of system user permissions. The audit revealed, among other things, frequent cases of weak passwords, shared user accounts, and failure to revoke permissions for former employees, creating vulnerabilities that could be exploited by attackers. Other dangerous practices observed include the opening of suspicious email attachments by untrained employees and the use of unsecured USB drives–the consequences of such behavior can be as serious as those of complex technical attacks, as they lead to malware infections or data leaks. Staffing and financial shortages are another aspect of organizational vulnerabilities. Small institutions (e.g., small municipalities, small businesses) often do not have the budget for cybersecurity specialists or modern security measures[15]. They are forced to rely on outdated systems that are easier to penetrate, or on the work of a single IT specialist performing multiple roles (without the possibility of specialization). Research in Polish local governments has shown that the most frequently cited problem in ensuring security is precisely the limitation of financial resources, which hinders both the purchase of technical solutions and the hiring of experts. In addition, some entities still do not conduct regular risk analyses or security audits–for example, almost 25% of municipalities in the study by Chodakowska et al. (2022)[16] admitted that it does not conduct a formal risk analysis of the loss of confidentiality, integrity, and availability of information, often justifying this by a lack of need or resources. Organizational gaps are also evident in the incomplete implementation of existing regulations. Despite the KSC Act being in force, some entities have not appointed a cybersecurity contact person or do not report incidents–the study cited showed that 44% of agencies that experienced incidents did not report them to the relevant authorities. Some organizations may be reluctant to disclose breaches for fear of consequences or loss of

14 M. van Haastrecht, B. Yigit Ozkan, M. Brinkhuis & M. Spruit, *Respite for SMEs: a Systematic Review of Socio-Technical Cybersecurity Metrics.* Applied Sciences 2021, No 11(15), p. 1

15 A. F. Ruggiero, T. D. Owusu & J. J. Staley, *Ransomware in local government: Risk factors…*, op. cit., pp. 183–191.

16 A. Chodakowska, S. Kańduła & Przybylska, *Cybersecurity in…*, op. cit., pp. 161–192.

reputation, which distorts the overall picture of threats and hinders the response at the national level. To sum up the threat analysis: the country faces both sophisticated external attacks and internal weaknesses in its own structures. Attacks on critical infrastructure and ransomware can cause direct crises and losses, disinformation undermines the foundations of public trust, and organizational gaps increase vulnerability to all of the above threats. Awareness of these threats is the starting point for designing adequate defense strategies.

Defense strategies

An effective national cybersecurity defense strategy must be multi-layered and comprehensive. There is no single remedy–a combination of legal, organizational, technical, and educational measures is needed, as well as close cooperation between the public and private sectors and citizens. The key pillars of a cyber defense strategy in relation to the previously identified threats are presented below.

Legal and institutional framework

The basis for defense is appropriate law and institutional structures. In implementing the NIS Directive, Poland established a National Cybersecurity System with clearly defined roles and procedures. The KSC Act obliges critical infrastructure operators and other key entities to maintain minimum security standards and to report and respond to incidents quickly[17]. This ensures that there is a formal response path in case of an incident: detection, notification of CSIRT, remedial action, and notification of other potentially affected entities. CSIRT teams act as first responders in cyber security – they analyze reports, support victims of attacks in restoring system functionality, and publish warnings about new threats. It is important to continuously improve their technical capabilities (e.g., investments in attack detection systems, development of threat intelligence) and ensure the rapid flow of information with private and foreign entities.

Another element is the state strategy – a strategic document setting out objectives and actions for the next few years. The current Cybersecurity Strategy of the Republic of Poland 2019–2024 emphasizes, among other things, the development of national incident response capabilities, the protection of critical infrastructure, the building of public awareness and competence, and international cooperation. The implementation of the strategy is coordinated by the Government Plenipotentiary for Cybersecurity, and progress is monitored. This type of document ensures an integrated approach, e.g., it links military issues (cyber defense in the Armed Forces) with civil issues (protection of administration networks) and the economy (increasing the resilience of infrastructure companies). Another important institutional

17 T. Baranovska, V. Savitskyi, M. Serbov, Y. Stoliar & Krutik, *The impact of cybercrime…*, op. cit., pp. 33–42.

initiative in Poland was the creation in 2022 of a Cyber Defense Forces component within the Armed Forces. These units (subordinate to the Cyber Defense Forces Component Command) are responsible for defensive and offensive actions in cyberspace for the purposes of national defense. Their existence strengthens the potential to respond to serious attacks (especially those sponsored by foreign countries) and enables active counteraction to threats within the framework of military operations. The combination of civilian (CERT/CSIRT) and military expertise in cybersecurity increases the state's ability to deter aggressors – it signals that Poland is not only capable of defending itself, but also of identifying the perpetrators of attacks and responding to them, including through legal measures or potential counterattacks (within the framework of international law).

Technical protection and best practices

At the operational level, it is crucial to implement specific technical measures and procedures that will make it difficult for attackers to achieve their goals. This is where the aforementioned standards and best practices come in handy. Every institution should implement multi-layered protection (*defense in depth*) – starting with network security (firewalls, intrusion detection systems), through workstation and server protection (up-to-date antivirus/EDR software, regular vulnerability patching), to data backup mechanisms and business continuity procedures (disaster recovery). In recent years, particular emphasis has been placed on access and identity management – for example, the implementation of two-factor authentication (2FA) for access to critical systems makes it significantly more difficult for attackers to take control even if passwords are leaked. Equally important is network segmentation (so that, for example, the infection of one computer does not immediately give access to the entire office network) and strict control of permissions (granting users only the minimum access necessary in accordance with the *least privilege* principle). Compliance with such rules could prevent many incidents reported by the NIK – for example, rigorous account management would eliminate the problem of universal passwords or active accounts of former employees.

In the context of ransomware, a technical defense strategy must include regular backups of critical data and systems and their secure storage (e.g., offline). This ensures that even if data is encrypted, the institution can restore its operations without paying a ransom. Many organizations that have fallen victim to ransomware have managed to recover thanks to backups. In addition, systems that detect unusual behavior indicative of a ransomware attack (e.g., mass file encryption operations) and automatically block such processes are becoming increasingly common. It is also essential to test your own security measures through audits and penetration tests. This allows you to identify vulnerabilities before a potential attacker does. For small entities that do not have their own experts, cooperation with external security auditors is a good solution – it is suggested, for example, that local governments could

use the services of specialists or certified providers (or even transfer some services to a cloud managed by trusted operators) to increase their level of data protection. This approach, while raising questions about trust in external partners, can be cost-effective and organizationally efficient for entities with limited resources. a large cloud provider is able to provide a level of security that is difficult to achieve locally. In summary, technical defenses must keep pace with threats: regular updates, patching vulnerabilities, monitoring systems, and contingency planning (backup, recovery) are the foundation of cybersecurity for any institution. Government policy should support the implementation of best practices, e.g. through the issuance of sectoral security guidelines, product certification (activities in this area are carried out, among others, by the EU Agency for Cybersecurity ENISA) or funding programs to increase security in critical sectors.

Cooperation between sectors

Cooperation between the public, private and civil sectors is absolutely crucial in the context of national cybersecurity. This is because a significant part of critical infrastructure and services (such as energy, telecommunications, banking) is owned or operated by private entities. The state is not able to secure the entire national cyberspace on its own–partnerships with businesses and the active involvement of citizens are needed.

At the national level, an example of cooperation is the creation of the Polish Cybersecurity Forum, a platform for the exchange of information between the administration, critical infrastructure operators, and experts. In addition, under the KSC Act, each key service operator is required to designate persons to liaise with the relevant authorities and CSIRTs, creating a network for cooperation and communication in the event of an incident. At the EU level, there is the NIS Cooperation Group, where representatives of member states and CERT teams exchange knowledge about threats and best practices. The NIS and NIS 2 Directives formalize this EU cooperation as one of the pillars of common digital security.

In the public sector, the concept of public-private partnerships (PPPs) in the field of cybersecurity is increasingly being promoted. This involves, for example, government agencies cooperating with technology companies to share information on threats (known as *cyber threat intelligence sharing*), organize joint simulation exercises, or even set up sector-specific information sharing and analysis centers (ISACs). This enables companies to respond more quickly to warnings issued by the authorities, while the state gains insight into the situation beyond its own systems. This type of cooperation is facilitated by the establishment of voluntary incident reporting mechanisms by the private sector – in Poland, digital service providers (e.g., large internet platforms) are also subject to reporting obligations for serious incidents, which brings them closer to public sector standards. At the local level, it is worth creating partnerships between local governments – for

example, neighboring municipalities can share knowledge, jointly hire a security specialist, or co-finance security systems. Such solutions allow for economies of scale – a single small municipality may not have the resources for a full-time cyber team, but several together can. Horizontal cooperation can also involve the exchange of good practices and experiences from incidents so that other entities can learn from each other's mistakes. The third segment is society – citizens who are both potential victims of cyberattacks (e.g., phishing) and the first line of defense (through their conscious behavior). Raising public awareness of cybersecurity is a strategic defense measure. Educational campaigns on phishing recognition, strong passwords, online privacy, and critical thinking about information (fact-checking, fake news recognition) can significantly reduce the effectiveness of hostile actors. As experts point out, education is key to exposing weaknesses and promoting good practices in cybersecurity[18]. The state should invest in training programs–both for its own officials (e.g., mandatory cyber hygiene training in the administration) and for citizens (e.g., through the education system–elements of digital and media education in schools). a society that is more resistant to manipulation and cautious online is an important protective layer against social engineering attacks and disinformation campaigns. Of course, it should be remembered that too much centralization or excessive state interference can also be undesirable – autonomous action by local and private entities is valuable. Cybersecurity is a public good that is best protected through joint efforts. The state can act as a coordinator and catalyst: conducting audits, identifying gaps (but not necessarily punishing immediately – it is more important to fix weaknesses), and sharing resources (e.g., offering smaller entities technical support or access to state security platforms).

Incident preparedness and resilience

Even the best prevention cannot eliminate the risk of an incident 100%, which is why preparation for attacks and ensuring resilience are key elements of the strategy. This means that institutions must have business continuity plans (BCP) and incident response plans (IRP) in place. Regular simulation exercises (*drills*) – e.g., backup system restoration tests, malware detection response scenarios, or *table-top* exercises for management – allow you to check whether your staff knows what to do and what decisions to make in a crisis situation. At the national level, large-scale cybersecurity exercises are organized (in Poland, these include Cyberyoyo, Cyber-Poligon, etc.), which involve various services and the private sector in joint training to respond to complex attacks. This allows weak points in coordination and communication to be identified before a real incident occurs.

18 T.T.P. Cortese, J.F.S.d. Almeida, G.Q. Batista, J.E. Storopoli, A. Liu, T. Yigitcanlar, *Understanding Sustainable Energy…*, op. cit., pp. 3.

Resilience also means the ability to quickly restore key functions after an attack. In practice, if, for example, a hospital is attacked by ransomware, it should have procedures in place to switch to manual mode or alternative systems to ensure continuity of patient care. Public administrations should ensure that they have the ability to switch services in an emergency, for example by having backup servers (even offline) on which basic e-services can be run if the main data centers are down. Diversification and redundancy are classic security approaches that are also used in IT – you should not keep all your resources in one place or allow single points of failure to exist.

International cooperation in responding to cross-border incidents is also extremely important. Cyberattacks rarely stop at a single country's border – malware spreads globally, and botnets attacking services in Poland can be controlled from abroad. That is why Poland actively participates in NATO and EU cyber defense initiatives. NATO has, among other things, the Cyber Defense Center of Excellence (CCDCOE) in Estonia, known for its Locked Shields exercises, in which Polish specialists also participate, learning from international partners. In the event of a serious attack, Poland can count on allied solidarity mechanisms (Article 5 of the North Atlantic Treaty potentially also covers cyber attacks if their effects are serious) and on the assistance of specialized units, such as NATO Cyber Rapid Reaction Teams. This international cooperation is part of the defense strategy–it also acts as a deterrent (the aggressor knows that an attack on one country may be met with a response from many).

Recommendations

An analysis of threats and current strategies allows us to formulate a number of recommendations to strengthen cybersecurity as an element of national security. The most important recommendations are presented below:

- Integrated strategic approach: a holistic cybersecurity strategy combining civil and military, national and international aspects should be continued and developed. The new strategy (post-2024) should take into account the experience of recent years and the implementation of the NIS 2 Directive, ensuring consistency between the actions of all actors involved.
- Strengthening the legal framework: It is recommended that the NIS 2 Directive be swiftly transposed into national law and that the Act on Cybersecurity be amended to cover a larger number of sectors and entities relevant to security (e.g., county-level local government, the chemical sector, and the space industry). The law should also provide for mechanisms for effective enforcement of obligations (audits, incident reporting) without excessive administrative burden.
- Increased funding and resources: The government should provide additional funding for cybersecurity in the public sector, especially for local government units and small government agencies, which are currently facing financial

difficulties in meeting all requirements[19]. This could take the form of dedicated funds, grants, or EU operational programs supporting investments in digital security (e.g., system upgrades, training, hiring experts). These investments should be treated similarly to national defense spending.

- Staff development and education: It is necessary to intensify programs for training cybersecurity specialists, both at the higher education level (more courses and places in IT studies with a specialization in security) and through certified professional training. For public administration, it is worth implementing a system for confirming competences (e.g., mandatory cybersecurity certificates for system administrators in government offices). In addition, public education on the basics of cyber hygiene and countering disinformation should become part of the state's information policy (public campaigns, school programs, cooperation with the media). Raising awareness will minimize the impact of the human factor as the weakest link in security[20].
- Improving cooperation and communication: It is recommended to establish formal channels for the exchange of information on incidents between the public and private sectors, e.g. by launching a national alert exchange platform accessible to operators of essential services and other interested companies. The state may also encourage the creation of industry-specific ISACs in sectors such as finance, energy, and transportation, where private entities jointly analyze threats. At the local government level, mechanisms encouraging the sharing of security specialists (e.g., a county employing an expert serving several nearby municipalities) should be considered.
- Regular audits and resilience tests: The government should finance and organize periodic cybersecurity audits of public institutions (especially at the local level) to detect and remove the weakest points. It is important that these audits are advisory rather than punitive in nature–the goal is to improve the situation, not to punish mistakes. At the same time, simulation exercises involving various entities (e.g., a nationwide exercise to respond to a massive ransomware attack on critical infrastructure) should be conducted to test procedures in conditions close to real life.
- Combating disinformation: As part of the state security system, capabilities to monitor and counter disinformation campaigns should be identified and developed. It is recommended that a permanent analytical group (including media experts, sociologists, psychologists, and IT specialists) be established to monitor narratives that threaten the country's information security. Its work should result in rapid corrections and statements issued by state authorities and cooperation with online platforms to limit the reach of harmful content (while respecting freedom of speech). In the long term, building social resilience through media

19 A. F. Ruggiero, T. D. Owusu & J. J. Staley, *Ransomware in local government: Risk factors…*, op. cit., pp. 183–191.

20 M. van Haastrecht, B. Yigit Ozkan, M. Brinkhuis & M. Spruit, *Respite for SMEs: a Systematic Review of Socio-Technical…*, op. cit., p. 2

education and the promotion of critical thinking is the best strategy for defending against disinformation.

- International coordination: Poland should continue to actively participate in EU and NATO initiatives on cybersecurity, share information on threats, and draw on the expertise of its allies. It is worth seeking to intensify regional cooperation (e.g. within the Visegrad Group or the Three Seas Initiative) on the exchange of information about attacks, as cyber campaigns often affect countries in our region simultaneously. In addition, it is recommended to organize joint international exercises and develop cybersecurity mutual assistance mechanisms in case of a serious incident exceeding the defense capabilities of a single country.
- The implementation of the above recommendations will strengthen the state's cyber resilience. It should be remembered that cyber threats will intensify with advancing digitization – the development of Smart Cities, 5G networks, and the Internet of Things increases the potential attack surface and poses new challenges for defenders[21]. Therefore, continuous improvement and adaptation of strategies is essential – cybersecurity is a process, not a state that can be achieved once and for all.

Summary

Cybersecurity in the 21st century is emerging as one of the pillars of national security, alongside traditional domains such as military defense and internal security. The analysis presented in this article shows that threats from cyberspace–attacks on critical infrastructure, ransomware, disinformation, and internal organizational vulnerabilities–have the potential to cause serious crises and destabilize the state. The experiences of recent years (both global and domestic) confirm that no modern country can ignore the issue of cybersecurity.

Poland has taken significant steps by creating a legal framework (the KSC Act, strategies) and institutions responsible for cybersecurity. Nevertheless, much remains to be done, especially at the level of practical implementation of objectives and strengthening the weakest links. Research on the state of cybersecurity in local governments points to the need to raise awareness, improve the implementation of policies and procedures, provide regular training, and improve cooperation between entities. a positive trend is the growing international and cross-sector cooperation–cyber threats are increasingly seen as a common challenge requiring a joint response. The main conclusion of the analysis is the need for an integrated approach to cybersecurity in the state strategy. This means simultaneously strengthening technical defenses, developing human competencies, improving laws and procedures, and building a broad coalition for a secure cyberspace–from the government, through the private sector, to a risk-aware civil society. Only such a holistic approach will

21 K. M. Hou, X. Diao, H. Shi, H. Ding, H. Zhou & C. de Vaulx, *Trends and challenges in AIoT/IIoT/IoT implementation*, Sensors 2023, No 23(11), p. 11.

effectively minimize the risk of cyberattacks and limit their impact, making the state more resilient to the challenges of the 21st century.

Ultimately, cybersecurity is a continuous process: it requires ongoing threat assessment, strategy adaptation, and rapid response to emerging new attack techniques. a state that treats cyberspace as an integral part of its security domain must invest in its protection as intensively as it does in traditional defense forces. The price of neglect in this area can be very high, as evidenced by statistics (annual increases in the number of incidents by tens of percent) and high-profile incidents in recent years. It can therefore be argued that ensuring national security in the 21st century is inextricably linked to ensuring cybersecurity. According to this thesis, all efforts to raise the level of cyber protection – legal, organizational, technical, and educational – are an investment in the broader security and stability of the state.

Bibliography

Ustawa z dnia 5 lipca 2018 r. *O krajowym systemie cyberbezpieczeństwa* Dz. U. 2018 poz. 1560 z późń. zm.

Ruggiero, A. F., Owusu, T. D., & Staley, J. J. (2022). *Ransomware in local government: Risk factors, vulnerabilities, and exploitation during a global pandemic*. Issues in Information Systems, 23(4).

Ali, H., Elzeki, O. M., & Elmougy, S. (2022). *Smart attacks learning machine advisor system for protecting smart cities from smart threats*. Applied Sciences, 12(13), 6473.

Baranovska, T., Savitskyi, V., Serbov, M., Stoliar, Y., & Krutik, Y. (2024). *The impact of cybercrime on state and institutional security: Analysis of threats and potential protection measures*. Economic Affairs, 69(Special Issue).

Chodakowska, A., Kańduła, S., & Przybylska, J. (2022). *Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done*. Lex Localis – Journal of Local Self-Government, 20(1),

Cortese, T.T.P.; Almeida, J.F.S.d.; Batista, G.Q.; Storopoli, J.E.; Liu, A.; Yigitcanlar, T. *Understanding Sustainable Energy in the Context of Smart Cities*: a PRISMA Review.Energies 2022, 15, 2382.

Fordoński, R., (2019) *WannaCry ransomware cyberattack as violation of international law* Uniwersytet Warmińsko-Mazurski, Studia Prawnoustrojowe (44)

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). *Understanding local government cybersecurity policy: a concept map and framework*. Information, 15(10).

van Haastrecht, M., Ozkan, B. Y., Brinkhuis, M., & Spruit, M. (2021). *Respite for SMEs: a systematic review of socio-technical cybersecurity metrics*. Applied Sciences, 11(15), 6909.

Hou, K. M., Diao, X., Shi, H., Ding, H., Zhou, H., & de Vaulx, C. (2023). *Trends and challenges in AIoT/IIoT/IoT implementation*. Sensors, 23(11), 5074.

Sophos. (2023). *The State of Ransomware in State and Local Government 2023*. Retrieved from Sophos News (news.sophos.com).

Terlecka-Maciejewska, M. (2024). *Cybersecurity in Polish security system*. Zeszyty Naukowe Politechniki Śląskiej, seria Organizacja i Zarządzanie, 198(2024).

https://sophos.com The State of Ransomware in State and Local Government 2023. Retrieved from Sophos News. – dostęp 27.04.2025 r.)

https://mazovia.pl/pl/bip/komunikaty/incydent-cyberbezpieczenstwa (dostęp 28.04.2025 r.)

About the Author

Dawid Kądzioła is a university lecturer and a PhD candidate at the University of Agriculture in Kraków. His academic interests include mechanical engineering, ergonomics, and machine design. He is a graduate of the Police Academy in Szczytno, majoring in Internal Security. His second field of scientific interest is cybersecurity in ICT systems. He is a certified Information Security Management System (ISO 27001) auditor and a cybersecurity officer for essential services in accordance with ISO 27001 and ISO 22301 standards. He also holds the title of Level II Cybersecurity Officer awarded by the Polish Institute of Internal Control. a police officer for over 22 years, he is currently affiliated with the Communication and IT Bureau of the General Police Headquarters in Warsaw.

Marek Przybyła, MA
University and MA in Logistics from the Military University of Technology
marek_przybyła@yahoo.com
ORCID: 0009-0007-0044-4495

DOI: 10.26410/SF_2/25/8

COUNTERING DISINFORMATION AS AN ELEMENT OF COMBATING CYBER THREATS AGAINST THE REPUBLIC OF POLAND

Abstract

The aim of this paper is to characterise the phenomenon of disinformation as one of the primary cyber threats undermining the security system of the Republic of Poland. Ensuring information security and cybersecurity is among the strategic priorities of the European Union. Disinformation constitutes a key instrument in hybrid operations, which are particularly prominent today, especially in the context of Russian activity. The near-revolutionary pace of technological advancement has enabled the Russian Federation to refine its disinformation campaigns, prompting the European Union, among others, to take action to counter this phenomenon. The main objective of the author is to present academically grounded benefits resulting from the development of effective methods to combat disinformation–regarded as one of the most urgent and significant challenges to Poland's information security. The solutions proposed in this publication may serve as a point of departure for further analysis, decision-making, legislative amendments, or the drafting of additional reports in this area. The paper relies on theoretical research methods. The reflections presented suggest that combating cyber threats requires the development of a system composed of effective processes to counter such risks–processes that, in turn, necessitate cooperation between state and private entities as well as society at large. The conclusions drawn may contribute to reducing the level of risk and enhancing the level of information security in the Republic of Poland.

Keywords

Cybersecurity, disinformation, fake news, fact-checking, microtargeting

Introduction

A fundamental component of the functioning of a state's overall security system is the identification of all types of threats, including cyber threats, which may pose risks, among others, to individuals holding senior positions within the government[1]. It is difficult nowadays to dispute the assertion that "cybersecurity is of vital importance not only to national prosperity and security, but also to the very functioning of our democracy, our freedoms, and our values[2]. The "National Security Strategy of the Republic of Poland", published in 2020, indicates that the neo-imperial policy of the Russian Federation undermines the foundations of the European security system. Russia pursues its objectives without resorting to military force by engaging in sub-threshold activities (hybrid operations[3]) through non-military means. With reference to cyberspace[4] and the information space, these include, among others, cyberattacks, disinformation, and manipulation[5]. It is not only Ukraine[6], that has fallen victim to Russian hybrid operations conducted in cyberspace, but also the Euro-Atlantic community. Hybrid operations in cyberspace involve planned and coordinated actions combining various forms of pressure, carried out either through a state's own resources or with the involvement of external actors, such as politically motivated hacktivists[7] (often referred to as cyber warriors), as well as through the exploitation of national, ethnic, or religious minorities. Hybrid activities in cyberspace typically include the simultaneous execution of disinformation campaigns and unconventional attacks within the information space. The activity of so-called cyber armies typically emerges during armed conflicts and international crises[8].

1 T. Goryca, *Selected Operational and Intelligence Activities as Elements of Bodies*, *Security Forum*, no. 1, 2024, WSB Academy Press, Dąbrowa Górnicza, p. 58.

2 Proposal for a Regulation of the European Parliament and of the Council on ENISA, repealing Regulation (EU) No 526/2013, and on cybersecurity certification in the field of information and communication technologies (OJ EU C 227/13 of 28.6.2018).

3 The underlying assumption of Russia's hybrid warfare is the weakening of the adversary's defensive potential – a form of so-called sub-threshold aggression carried out during an official state of peace through sabotage and information operations. Source: M. Wojnowski, *Mit „wojny hybrydowej". Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku*, [in:] *Przegląd Bezpieczeństwa Wewnętrznego. Wojna hybrydowa – Wydanie Specjalne*, Wydawnictwo Agencji Bezpieczeństwa Wewnętrznego, Wiązowna 2015, no. 15, p. 23.

4 Cyberspace is understood as a virtual domain for the processing and exchange of information, formed by ICT systems, within which interactions occur between networks and users.

5 *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2020, pp. 6–8.*

6 See more in: S. Tomaszewski, *Media elektroniczne jako instrument walki informacyjnej*, [in:] W. Fehler (ed.), *Informacyjny Wymiar Bezpieczeństwa Państw i Jednostek*, Wydawnictwo Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2021, p. 240.

7 A term derived from the combination of two words: hacker and activist.

8 T. Nowak, *Działania hybrydowe w cyberprzestrzeni prowadzone przez Rosję jako zagrożenie dla bezpieczeństwa euroatlantyckiego*, [w:] M. Banasik, A. Rogozińska (red.), *Zagrożenia Federacji Rosyjskiej i Bezpieczeństwo Międzynarodowe*, Wydawnictwo Difin SA, Warszawa 2020, s. 73.

Methodology

The central problem addressed in this article is expressed in the form of the following research question: How can disinformation be effectively and efficiently countered in the process of combating cyber threats against the Republic of Poland?

During the research process, theoretical research methods were employed, including: analysis (which enabled the identification of individual components and distinctive features of the subject under study), synthesis (which allowed for the establishment of relationships between the various elements of the subject), definition (which facilitated the clarification of terms related to the research topic), and inference (which supported the formulation of new conclusions concerning the subject under investigation)[9].

The analysis was based on the available literature related to the subject of the research[10], In particular, the analysis encompassed Polish and foreign-language monographs, printed academic articles, online sources, as well as specialised textbooks, manuals, guidelines, and applicable legal regulations.

Disinformation as a Contemporary Form of Cyber Threat

According to T. Nowak, the most significant tools employed by Russia against Euro-Atlantic countries between 2014 and 2019 included: disinformation [11], manipulation [12], fake news[13], information disruption, cyberattacks, and cyberespionage[14]. Disinformation campaigns constitute a crucial component of hybrid operations conducted in cyberspace. By employing manipulation, the Russian Federation constructs a negative image of the authorities and societies of targeted states, while also undermining the reputation of their armed forces. To this end, among other methods, highly impactful fake news is generated. At the end of December 2019, a fake

9 See more in: *Bezpieczeństwo. Teoria–Badania–Praktyka*, A. Czupryński, B. Wiśniewski, J. Zboina (scientific eds.), Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego – Państwowy Instytut Badawczy, Józefów 2015, p. 32.

10 See more in: *Nauki o bezpieczeństwie. Wybrane problemy badań*, A. Czupryński, B. Wiśniewski, J. Zboina (scientific eds.), Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego – Państwowy Instytut Badawczy, Józefów 2017.

11 In the traditional sense, disinformation refers to false information that has been deliberately and intentionally fabricated, as well as to planned actions involving the transmission of untrue content to an adversary. The objective of disinformation efforts is to influence the decision-making processes of another state's authorities. Such activities may be carried out through mass media or by means of operational measures undertaken by intelligence services. Source: P. Bączek, *Dezinformacja jako zagrożenie dla bezpieczeństwa informacyjnego współczesnych społeczeństw*, *Security Review*, Wydawnictwo Instytut Analizy Ryzyka Sp. z o.o., Rzeszów 2020, no. 4 (17), pp. 9–11.

12 Most broadly, manipulation can be defined as "any covert, intentional, and deliberate influence exerted on recipients in order to affect their attitudes and, ultimately, their behaviour." Source: M. Golka, *Bariery w komunikowaniu i społeczeństwo (dez)informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2008, p. 112.

13 Fake news can be defined as "information intended to deliberately and knowingly mislead the recipient in order to gain image-related, financial, psychological, propaganda, political, or economic benefits." Source: B. Rejman, K. Rejman, *Fake news jako narzędzie działań dezinformacyjnych a bezpieczeństwo współczesnych systemów społeczno–ekonomicznych*, [in:] K. Rejman, M. Wilczyńska, J. Wołejszo (eds.), *Bezpieczeństwo Informacji Wobec Współczesnych Zagrożeń*, Wydawnictwo Kaliskie Towarzystwo Przyjaciół Nauk, Kalisz 2023, p. 216.

14 T. Nowak, *Działania hybrydowe w cyberprzestrzeni…*, op. cit., p. 74.

news story was disseminated via bots, reproducing an article from *Russia Today* which claimed that Poland had attempted to pressure Belarus into abandoning its cooperation with Russia and moving closer to NATO. The authors of the manipulated information exploited the widely known view that the eastward expansion of NATO infrastructure poses a military threat to Russia[15]. Moreover, during the peak of military operations in the Donbas region, Facebook posts were published targeting residents of western Ukraine, encouraging them to leave the country for economic reasons, with Poland being the primary destination. Additionally, these posts stirred anti-government sentiment among the population of Lviv by recalling that Lviv was once a Polish city. Other content included links to external websites about visa-free travel between Ukraine and EU member states, as well as information on how to find employment in Poland[16]. Among the most significant consequences of Russian hybrid activities in cyberspace are: the discrediting of EU and NATO member states; the fuelling of antagonisms rooted in historical experiences; efforts to sow division and obstruct cooperation and decision-making processes; and the consolidation of pro-Russian groups within the target countries[17].

Ensuring information security, ICT security (cybersecurity), and operational[18] continuity is one of the strategic priorities of the European Union.

To this end, in 2015, an action plan was established in response to Russian disinformation. As a result, a working group called the *East StratCom Task Force* (ESTF) was created. The ESTF consists of a team of analysts and experts who monitor the course of pro-Russian disinformation campaigns[19]. There is a visible trend indicating that Brussels is strengthening its capabilities in identifying and countering disinformation. Efforts have been undertaken to build structures aimed at enhancing situational awareness and supporting decision-making processes.

Since 2014, there has been a significant increase in offensive activity in cyberspace carried out by entities that are either part of Russian state structures or act on their behalf or in their interest, conducting large-scale disinformation campaigns primarily targeting NATO and EU member states. It is worth noting that this phenomenon is not limited to the Russian context. Similar actions are undertaken by other international actors aspiring to global or regional power status. Well-documented examples include China (Karásková 2020) and Iran (Kasapoglu 2020). It should be

15 T. Nowak, *Działania hybrydowe w cyberprzestrzeni…*, op. cit., pp. 78–79.

16 R. DiResta, S. Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*, ed. Stanford Cyber Policy Center, Stanford 2019, pp. 54–56.

17 T. Nowak, *Działania hybrydowe w cyberprzestrzeni…*, op. cit., p. 83.

18 Szerzej, T. Goryca, *Risk and threats in protective measures of the units responsible for security of executive states bodies*, „Security Forum" 2022, nr 1, Wydawnictwo Akademia WSB, Dąbrowa Górnicza 2022.

19 T. Nowak, *Polityka Unii Europejskiej w latach 2014-2019 wobec działań hybrydowych Federacji Rosyjskiej*, [w:] M. Banasik, A. Rogozińska (red.), *Zagrożenia Federacji Rosyjskiej i Bezpieczeństwo Międzynarodowe*, Wydawnictwo Difin SA, Warszawa 2020, s. 135. See more in: T. Goryca, Risk and Threats in Protective Measures of the Units Responsible for Security of Executive State Bodies, Security Forum 2022, no. 1, Wydawnictwo Akademia WSB, Dąbrowa Górnicza 2022. T. Nowak, Polityka Unii Europejskiej w latach 2014–2019 wobec działań hybrydowych Federacji Rosyjskiej, [in:] M. Banasik, A. Rogozińska (eds.), Zagrożenia Federacji Rosyjskiej i Bezpieczeństwo Międzynarodowe, Wydawnictwo Difin SA, Warszawa 2020, p. 135.

emphasised that tools of informational influence and modern channels of information dissemination are used–albeit to varying degrees–by virtually all states across the world[20]. Admittedly, not all states engage in disinformation activities or employ fabricated information sequences. Moreover, information warfare is not exclusively the domain of state actors. Non-state entities are also active in this area–including terrorist organisations such as Daesh (ISIS) (Winter 2019)[21].

The development of effective methods for combating disinformation has become one of the most urgent and significant challenges facing contemporary science. At the same time, it is an exceptionally interdisciplinary issue, requiring intensive collaboration across the natural sciences, medical sciences, social sciences, and the humanities[22].

Countering Disinformation

In developing a framework for countering disinformation in Poland, it is essential to examine the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions – *Tackling online disinformation: a European approach* (April 2018), which outlines four fundamental pillars for combating disinformation on the Internet[23]:

- improving transparency regarding the origin of content and the means by which it is financed;
- promoting information diversity in order to foster users' critical thinking and support high-quality journalism;
- strengthening the credibility of information by indicating whether it can be trusted;
- developing coordinated actions involving broad engagement of public authorities, online platforms, advertisers, trusted fact-checking entities, journalists, and media groups[24].

---

20 There is a widely held view that AI (AI – an acronym formed from the initial letters of the term "artificial intelligence") will enable states, corporations, and organisations to spread false content more effectively–content that will appear credible. As a result, the problem of disinformation dissemination will become even more difficult to resolve. Source: P. Bączek, Wyzwania i zagrożenia dezinformacyjne w kontekście rozwoju sztucznej inteligencji, [in:] W. Fehler (ed.), Informacyjny Wymiar Bezpieczeństwa Państw i Jednostek, Wydawnictwo Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2021, p. 136.

21 R. Kupiecki, F. Bryjka, T. Chłoń, *Dezinformacja międzynarodowa – Pojęcie, Rozpoznanie, Przeciwdziałanie*, Wydawnictwo Naukowe Scholar, Warszawa 2022, p. 22.

22 J. Kuś, *Zjawisko dezinformacji z perspektywy psychologicznej: uwarunkowania i przeciwdziałanie*, [in:] K. Stasiuk-Krajewska, M. Wenzel (eds.), *Dezinformacja w czasach kryzysu*, Wydawnictwo Adam Marszałek, Toruń 2024, p. 77.

23 M. Danek, *Modele walki z dezinformacją: od restrykcji do współpracy*, [in:] M. Bernaczyk, T. Gąsior, J. Misiuna, M. Serowaniec (eds.), *Znaczenie nowych technologii dla jakości systemu politycznego – ujęcie politologiczne, prawne i socjologiczne*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2020, p. 143.

24 The media play a key role in shaping how we perceive the world around us. For many people, the Internet has become the primary tool for acquiring knowledge about the world, a natural environment for gaining experience and fulfilling social needs, as well as a means of effective communication and access to information on an unprecedented scale. Source: See M. Szulc, Manipulowanie informacją w sieci za pomocą fake newsów jako zagrożenie dla młodzieży, [in:] Psychologia Wychowawcza, Wydawnictwo Uniwersytet Gdański, Gdańsk 2020, vol. 599730, no. 17, pp. 140–157.

Moreover, the budget of the European External Action Service for combating disinformation was increased from €1.9 million to €5 million, and a *Rapid Alert System* was established. Co-developed by national contact points, this system enables real-time alerts regarding foreign disinformation campaigns[25]. On 14 June 2019, the European Commission published a report on the implementation of its action plan against disinformation. The report emphasised that significant progress had been made in identifying and countering disinformation, cooperating with online platforms, raising public awareness, and ensuring a relatively calm and secure conduct of the European elections[26]. Nevertheless, the problem of disinformation has not disappeared, and disinformation campaigns remain highly effective[27].

On 16 June 2022, the European Commission presented an enhanced Code of Practice on Disinformation, linked to the Digital Services Act, stating that disinformation has become a very serious threat capable of significantly impacting the political and social situation worldwide[28]. In recent years, there have been large-scale disinformation attempts, typically associated with major geopolitical events such as Russia's invasion of Ukraine in 2022 or the U.S. elections in 2016 and 2020. As early as 2016, it was demonstrated that disinformation accounted for over 70% of all circulated content in social media spaces. Moreover, it has been observed that disinformation can significantly suppress the potential for social innovation, which in turn may lead to a decline in a state's economic capacity[29].

In order to combat disinformation, it is essential to undertake systemic action within the broadly understood sphere of education. Such efforts must encompass all levels of the educational system–primary, secondary, and higher education. It would also be advisable to implement similar initiatives targeting older individuals, for instance those participating in lifelong learning programmes such as universities of the third age. a particularly important role in exposing fake news is played by media professionals, as well as members of the academic and expert communities. The responsibility of supporting the state in countering this phenomenon rests largely on their shoulders. It is worth considering whether cooperation should be established between state institutions and other entities responsible for education, with the aim of building infrastructure to fight fake news. It is also crucial to implement mechanisms that enable the rapid verification of potentially false information. Such analysis should take place at an expert level and be widely disseminated among the public. This practice is referred to as *fact-checking*. Fact-checking organisations are

25 M. Danek, *Modele walki z dezinformacją…*, op. cit., p. 144.

26 Tamże, s. 145.

27 The power of its dissemination is attributed to the rapid pace of technological advancement, widespread access to information, the speed at which it spreads, and its specific digital features such as editability, openness, interactivity, and high shareability. Source: K. Stasiuk-Krajewska, *Dezinformacja. Próba ujęcia dyskursywnego*, *Media – Kultura – Biznes*, Wydawnictwo Uniwersytet Gdański, Gdańsk 2023, vol. 1 (14), p. 56.

28 Such activity is less costly than conventional military confrontation, yet equally severe in terms of its consequences. Source: K. Janik, *Państwo, Polityka, Bezpieczeństwo Wewnętrzne*, Wydawnictwo Adam Marszałek, Toruń 2021, p. 57.

29 M. Danek, *Modele walki z dezinformacją…*, op. cit., s. 59.

institutions, associations, or groups of individual experts whose primary task is to verify the accuracy of public claims and information (e.g., the association *Demagog*). These organisations most commonly operate as part of newsrooms or as independent non-governmental organisations, and less frequently within academic institutions.

Fact-checking, understood as the professional verification of the authenticity of facts and information circulating in the media space, has become the most widespread method of combating disinformation. By definition, it is a process involving the assessment of the truthfulness of content conveyed in written and spoken messages that enter the public sphere and have been formulated within a specific context[30].

The most active fact-checking organisation is the *International Fact-Checking Network* (IFCN). Its main goal is to bring together individuals and institutions involved in combating disinformation and verifying facts, by facilitating networking, building collaborative frameworks through advocacy, organising various events, training sessions, conferences, expert meetings, and by providing financial support to entities engaged in fact-checking activities.

It is also worth examining the FactcheckEU project, which was initiated by 19 fact-checking entities from 13 countries with the aim of verifying information during the European Parliament elections. Another noteworthy initiative is the SOMA project (Social Observatory for Disinformation and Social Media Analysis) – launched by the European Commission in cooperation with five fact-checking organisations from Greece, Italy, and Denmark. Its objective is to promote campaigns aimed at combating disinformation and to organise training programmes for experts. The relevance of fact-checking organisations is evidenced by the fact that, in the first six weeks of the Russia–Ukraine conflict in 2022 alone, nearly 20,000 reports of disinformation were submitted through just one fact-checking project. Moreover, from the outbreak of the war until 31 August 2023, over 15 billion mentions related to Russian disinformation were recorded.

Educational efforts aimed at combating disinformation should also include media literacy education[31]. The primary normative act of the European Union concerning media education is the Audiovisual Media Services Directive (AVMSD) of 2018. It assigns responsibilities to various media market stakeholders in promoting and developing media literacy. It also obliges EU Member States to support the development of media-related competencies and implement appropriate measures in this regard, as well as to submit regular reports to the European Commission. For instance, France

30 M. Kowalska-Chrzanowska, P. Krysiński, N. Pamuła, *Metody i narzędzia budowania społecznej odporności na dezinformację: od fact-checkingu po edukację medialną*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2024, p. 72.

31 Researchers are divided on the issue of disinformation. Some perceive it as occurring exclusively on social media platforms, while others point to its presence in more traditional forms of mass communication–such as television, radio, and the press–as well as in private life and the political sphere. Sources: A. Khan, K. Brohman, S. Addas, *The Anatomy of "Fake News": Studying False Messages as Digital Objects*, *Journal of Information Technology*, ed. Sage, 2022, vol. 37, iss. 2, pp. 122–143; and *The Disinformation Age: Politics, Technology and Disruptive Communication in the United States*, eds. W. L. Bennet, S. Livingston, Cambridge University Press, Cambridge 2021, p. 28.

introduced the Act on Combating the Manipulation of Information of 22 December 2018, which imposes on internet platforms under French jurisdiction the obligation to fight the spread of false information, including through initiatives promoting media and information literacy[32]. In 2022, Italy launched a national centre for combating disinformation – the Italian Digital Media Observatory (IDMO) at Luiss Guido Carli University (LUISS), which forms part of a European network established at the initiative of eight Member States. The project is funded by the EU budget[33].

Poland lacks a coherent strategy regarding media literacy and the use of new media by young people. Nevertheless, the issue has received attention within the programmes of the Ministry of Education and Science and the Ministry of Digital Affairs. Media literacy education was introduced in 1999 in primary and lower secondary schools; however, the implementation of the programme proved inconsistent, and the media education curriculum was abandoned in 2008[34]. It is worth examining selected initiatives that support the fight against disinformation in Poland and worldwide: Akademia Fact-Checkingu, Demagog Educational Platform, #FakeHunter EDU, CovidHub EDU, MedFake, EUvsDisinfo, and Fake News & Elders.

NATO experts recommend that mass media analyse information and verify facts prior to publication or further dissemination, and educate the public about disinformation activities in online media by providing analyses and studies of various disinformation tactics and manipulation techniques. Government institutions, in turn, are advised to identify and expose sources of disinformation, which entails placing greater emphasis on analysing the information environment. Ultimately, this leads to faster identification of disinformation activities and their impact on public discourse[35].

At the individual level, actions should be taken that allow for at least partial differentiation between true and false content. The method by which the credibility of information can be verified is based on four fundamental elements: assessing the source, the fact, the image, and the timeliness. The International Federation of Library Associations and Institutions (IFLA) recommends eight key steps for verifying fake news:

- Check the source – the website's data, editorial details, domain ownership, and sources of funding;
- Check the authors – their actual identity, qualifications, and professional background;
- Check the date – the relevance and timeliness of the topic in relation to real-world events;
- Read beyond – do not rely solely on headlines;
- Consult additional sources of information;

32 M. Kowalska-Chrzanowska, P. Krysiński, N. Pamuła, *Metody i narzędzia budowania…*, op. cit., p. 100.
33 Ibid, p. 188.
34 Ibid, p. 145-146.
35 Ibid, p. 67.

- Avoid bias and refrain from judging based on personal prejudices;
- Determine whether it may be satire or a joke by checking other sources;
- Ask the experts – confront questionable claims and information by consulting professionals in the relevant field[36].

While the above recommendations cannot fully immunise individuals and groups against disinformation, efforts to combat disinformation should involve not only government institutions, security services, and organisations, but also individual citizens.

It is also worth noting the GANESA[37], programme, funded by the European Parliament, under which teaching scenarios were developed – including lesson plans, workshops, and seminar formats. The above are components of an educational process aimed at shaping attitudes in the younger generation that are desirable in a civic society, as well as supporting conscious, responsible, and well-informed decision-making in personal life. An example lesson plan has been proposed for upper secondary school students, focusing on counteracting disinformation. The primary objective of the class is to develop students' awareness of what fake news is and how to distinguish it from true information. An additional goal is to teach students the following mechanisms:

- verification of information in the media;
- critical selection of sources;
- distinguishing between the concepts of: manipulation, disinformation, post-truth, stereotype, information bubble, and virality[38];
- identifying the above phenomena in texts[39].

Moreover, a procedure for verifying information has been proposed:

- checking the source from which the information originates;
- reading the full content of the article rather than relying solely on the headline;
- checking who the author of the text is;
- paying attention to footnotes and annotations;
- analysing any accompanying images for signs of photomontage or manipulation;
- ensuring that the information being verified is not a joke or satire;
- thinking three times before sharing the information[40].

Well-developed fact-checking projects and effective efforts in the field of media education constitute essential components of the disinformation counteraction system. To this end, broad cooperation should be established between state institutions and other entities responsible for education, in order to build infrastructure for combating disinformation.

36 M. Kowalska-Chrzanowska, P. Krysiński, N. Pamuła, *Metody i narzędzia…*, op. cit., p. 64.

37 www.ganesa.uni.wroc.pl, [accessed 6 May 2025].

38 The tendency for an image, video, or piece of information to spread rapidly and widely from one internet user to another.

39 *Dialog w Unii Europejskiej – scenariusze zajęć dydaktycznych z zakresu…*, op. cit., s.103.

40 Tamże, s. 105.

Pitfalls in Combating Disinformation

The European Union defines disinformation as verifiably false or misleading information that is created, presented, and disseminated for economic gain or to intentionally deceive the public, and which may cause public harm. In relation to this definition, among the indicators that fall under the category of "public harm" are "threats to democratic political processes." One such threat is undoubtedly political advertising, which in recent years has been increasingly tailored to specific target audiences–meaning it is precisely targeted. The practice of targeting and microtargeting–i.e. directing messages at narrowly defined audience segments–originates from the advertising sector and involves adjusting the message to the specific needs of recipients. The use of microtargeting techniques during the U.S.[41] presidential campaign and the referendum that led to the United Kingdom's withdrawal from the European Union demonstrates that, in the political sphere, this practice can have serious consequences for public life. Microtargeting remains a phenomenon that has not yet been thoroughly studied in the context of Polish politics; however, it is becoming increasingly common due to the growing use of new technologies by politicians, which make such practices possible[42]. The Code of Practice developed by the European Commission includes a commitment requiring online platform operators to ensure that information concerning targeting and microtargeting is publicly accessible, and that users can find out why a given advertisement–including political advertising–is being directed specifically at them[43]. It is worth emphasising that the Polish legislator has not yet introduced any measure requiring the public disclosure of information regarding the targeting and microtargeting of political advertisements.

There are instances in which the fight against fake news takes the form of pursuing political interests[44] and significantly affects the restriction of freedom of expression online – for example, through the adoption of restrictive legislation or the implementation of tools that, under the guise of combating disinformation, are in fact used to surveil citizens[45]. While the blocking and removal of content promoting terrorism and extremism can – and indeed should – be considered legitimate, more controversial are cases such as that of Pakistan, where content deemed blasphemous or critical of the judiciary has been removed; Turkey, where statements

41 B. Trish *„Big Data under Obama and Trump: The Data-Fueled U.S. Presidency". Politics and Governance* (ISSN: 2183-2463), ed. Cogitatio Press, Lisbon 2018, vol. 6, s. 29-38.

42 K. Izdebski, *Walka z dezinformacją oraz przejrzystość reklam politycznych w przestrzeni internetowej*, [in:] M. Bernaczyk, T. Gąsior, J. Misiuna, M. Serowaniec (eds.), *Znaczenie nowych technologii dla jakości systemu politycznego – ujęcie politologiczne, prawne i socjologiczne*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2020, p. 170.

43 Ibid., p. 172.

44 In an era of information overload and a lack of effective verification mechanisms, it is difficult to determine whether statements made by a politician -statements that may even align with Russian propaganda – are deliberate acts or simply the result of unawareness of the risk that such remarks could be used contrary to the author's intent. Source: M. Marek, *Operacja Ukraina – Kampanie dezinformacyjne, narracje, sposoby działania rosyjskich ośrodków propagandowych przeciwko państwu ukraińskiemu w okresie 2013–2019*, Wydawnictwo Difin SA, Warszawa 2020, p. 128.

45 M. Danek, *Modele walki z dezinformacją…*, op. cit., p. 135.

defamatory of Mustafa Kemal Atatürk have been censored; or Russia, where content related to unauthorised protests or challenging the territorial integrity of the Russian Federation has been taken down. This should not, however, discourage efforts to combat the spread of false information in cyberspace, nor should it undermine recognition of the impact disinformation has on political and social systems[46]. One of the most prominent examples of disinformation spread within the Polish internet space is the case of the computer game Blue Whale, which was alleged to encourage children on a mass scale to commit suicide. The story, originally published by the newspaper The Sun and subsequently reported by Polish media (and, unsurprisingly, widely shared on social media), prompted a response from the Ministry of National Education, which issued a warning to schools. This situation highlighted how media exaggeration can influence the political decision-making process. The above example demonstrates that online disinformation poses a potential threat both to social security and to the functioning of the political system. However, the fundamental issue remains how to combat this phenomenon effectively without infringing upon freedom of expression[47]. The current pace of technological development–often described as the fastest in human history and referred to as a revolution–has resulted in a situation where political spheres and state institutions do not always keep up with the rate of change. As a consequence, the actions they undertake do not shape the emerging reality, but rather constitute a post-factum response[48].

In this context, it is worth noting the legal measures undertaken by Germany and France to combat fake news in cyberspace. On 1 January 2018, the restrictive provisions of Germany's Network Enforcement Act (NetzDG) came into force. The act imposes an obligation on social media platforms with more than two million users to promptly remove posts reported by users as inciting hatred. These platforms are required to delete such posts within 24 hours, although the deadline may be extended to seven days if the content is subject to dispute. Failure to comply may result in financial penalties of up to €50 million. The law was widely criticised by the then parliamentary opposition as well as by representatives of Facebook in Germany. In France, meanwhile, in accordance with earlier announcements by President Emmanuel Macron, the National Assembly passed a law in November 2018 that, during the pre-election period and throughout elections, obliges online platforms to publicly disclose the identity of entities purchasing sponsored political content, along with the amount of money spent for this purpose. As it soon turned out, the French government itself became a victim of this legislative solution when Twitter France announced it would not unilaterally determine which content qualified as political, and consequently blocked all such advertising in France – including a government-sponsored voter turnout campaign ahead of the European Parliament elections[49]. In Singapore, the authori-

46 Ibid., p. 136.

47 M. Danek, *Modele walki z dezinformacją…*, op. cit., p. 137.

48 Ibid., p. 138.

49 Ibid., pp. 139–140.

ties have implemented legislation containing a very broad definition of what may be arbitrarily classified as fake news. This includes, for example, statements that influence the outcome of presidential or parliamentary elections or referendums, as well as content that undermines public confidence in the performance of any duty, function, or power by the government or any other state authority. The dissemination of such content is punishable by a fine of up to 1 million Singapore dollars (approximately 735,000 USD) or up to ten years of imprisonment[50].

The above examples clearly demonstrate that combating disinformation in cyberspace is not an easy task and cannot be achieved through a single political decision or isolated political action. Countering cyber threats requires the creation of a system composed of effective processes aimed at mitigating such risks, which, in turn, necessitates cooperation between state institutions, private entities, and society as a whole.

Conclusions

Contemporary threats to national security also reside in cyberspace. Disinformation is a key tool used to weaken the defence capabilities of states. Since 2014, there has been a marked increase in offensive cyber activity carried out by entities operating within Russian state structures, or on their behalf, conducting large-scale disinformation campaigns primarily targeting NATO and EU member states. Among the most significant consequences of Russia's hybrid operations in cyberspace are the discrediting of EU and NATO member states, the fuelling of historical antagonisms, the pursuit of societal division, the obstruction of cooperation and decision-making processes, and the consolidation of pro-Russian circles within target countries.

The search for appropriate methods and effective means of ensuring both individual and collective security in the Republic of Poland has become a priority not only for national governments but also for international organisations[51].

In conclusion, it must be acknowledged that in order to enhance the level of state security, it is essential to develop a disinformation counteraction system that relies on close cooperation between state institutions, private actors, and society at large. Fact-checking initiatives have demonstrated that rapid responses to false content – as well as its removal from media and digital spaces – contribute to improving the overall security of the information creation and distribution system[52]. At the individual level, actions should be taken to enable the partial distinction between true and false content. The method for verifying the credibility of information is based on four fundamental elements: assessment of the source, the fact, the image, and the timeliness.

Disinformation on the internet poses a potential threat both to social security and to the functioning of the political system. a solution should be developed to ensure

50 M. Danek, *Modele walki z dezinformacją…*, op. cit., p. 134.

51 T. Goryca, *Theory and Practical Aspects of State Authorities Protection Organization*, *Security Forum* 2021, no. 2, Wydawnictwo Akademia WSB, Dąbrowa Górnicza 2021, p. 55.

52 Ibid., p. 14.

oversight of the targeting and microtargeting of political advertisements. To this end, the Code of Practice of the European Commission may serve as a reference, as it obliges online platform operators to make information on targeting and microtargeting publicly accessible, and to provide users with clear explanations as to why a given advertisement – including political advertising – is directed specifically at them.

In combating disinformation and in the field of media education, the state plays a key role. Actions in this area must encompass all levels of education – primary, secondary, and higher. a particularly important role is also played by media representatives, as well as members of the academic and expert communities, who bear the responsibility of supporting the state in countering disinformation. Cooperation should be established between state institutions and other entities responsible for education in order to build the necessary infrastructure to address this phenomenon. It is essential to introduce institutional and legislative systemic solutions that will, to some extent, immunise the state – and thus its citizens – against the growing spread of disinformation in the media.

Bibliography

Bączek P., *Dezinformacja jako zagrożenie dla bezpieczeństwa informacyjnego współczesnych społeczeństw*, *Security Review*, Wydawnictwo Instytut Analizy Ryzyka Sp. z o. o., Rzeszów 2020, no. 4 (17).

Bączek P., *Wyzwania i zagrożenia dezinformacyjne w kontekście rozwoju sztucznej inteligencji*, [in:] W. Fehler (ed.), *Informacyjny Wymiar Bezpieczeństwa Państw i Jednostek*, Wydawnictwo Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2021.

Bennet W. L., Livingston S. (eds.), *The Disinformation Age: Politics, Technology and Disruptive Communication in the United States,* Cambridge University Press, Cambridge 2021.

Chałubińska-Jentkiewicz K., *Droga do regulacji? Dezinformacja w przekazie medialnym*, [in:] K. Chałubińska-Jentkiewicz, M. Nowikowska, K. Wąsowski (eds.), *Media w erze cyfrowej. Wyzwania i zagrożenia*, Wydawnictwo Wolters Kluwer, Warszawa 2021.

Cyuńczyk F., Walka z dezinformacją w warunkach kryzysu praworządności, [in:] K. Stasiuk-Krajewska, M. Wenzel (eds.), Dezinformacja w czasach kryzysu, Wydawnictwo Adam Marszałek, Toruń 2024.

Czupryński A., Wiśniewski B., Zboina J. (eds.), *Bezpieczeństwo. Teoria–Badania–Praktyka,* Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego – Państwowy Instytut Badawczy, Józefów 2015.

Czupryński A., Wiśniewski B., Zboina J. (eds.), *Nauki o bezpieczeństwie. Wybrane problemy badań,* Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego – Państwowy Instytut Badawczy, Józefów 2017.

Danek M., *Modele walki z dezinformacją: od restrykcji do współpracy*, [in:] M. Bernaczyk, T. Gąsior, J. Misiuna, M. Serowaniec (eds.), *Znaczenie nowych technologii dla jakości systemu politycznego – ujęcie politologiczne, prawne i socjologiczne*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2020.

DiResta R., Grossman S., *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019*, ed. Stanford Cyber Policy Center, Stanford 2019.

Gliwa S., *Terroryści w sieci – media społecznościowe w służbie propagandy ISIS*, Wydawnictwo Towarzystwa Wiedzy Obronnej, Warszawa 2021.

Golka M., *Bariery w komunikowaniu i społeczeństwo (dez)informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2008.

Goryca T., *Risk and Threats in Protective Measures of the Units Responsible for Security of Executive State Bodies*, *Security Forum* 2022, no. 1, Wydawnictwo Akademia WSB, Dąbrowa Górnicza 2022.

Goryca T., *Selected Operational and Intelligence Activities as Elements of State Bodies*, *Security Forum* 2024, no. 1, Wydawnictwo Akademia WSB, Dąbrowa Górnicza 2024.

Goryca T., *Theory and Practical Aspects of State Authorities Protection Organization*, *Security Forum* 2021, no. 2, Wydawnictwo Akademia WSB, Dąbrowa Górnicza 2021.

Izdebski K., *Walka z dezinformacją oraz przejrzystość reklam politycznych w przestrzeni internetowej*, [in:] M. Bernaczyk, T. Gąsior, J. Misiuna, M. Serowaniec (eds.), *Znaczenie nowych technologii dla jakości systemu politycznego – ujęcie politologiczne, prawne i socjologiczne*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2020.

Janik K., *Państwo, Polityka, Bezpieczeństwo Wewnętrzne*, Wydawnictwo Adam Marszałek, Toruń 2021.

Kaczmarczyk B., Wiśniewski B., Gwardyński R., *Security of an Individual*, *Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy*, no. 3 (28) 2018, Legnica 2018.

Khan A., Brohman K., Addas S., *The Anatomy of "Fake News": Studying False Messages as Digital Objects*, *Journal of Information Technology*, Sage, 2022, vol. 37, iss. 2.

Kowalska-Chrzanowska M., Krysiński P., Pamuła N., *Metody i narzędzia budowania społecznej odporności na dezinformację: od fact-checkingu po edukację medialną*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2024.

Kupiecki R., Bryjka F., Chłoń T., *Dezinformacja międzynarodowa – Pojęcie, Rozpoznanie, Przeciwdziałanie*, Wydawnictwo Naukowe Scholar, Warszawa 2022.

Kuś J., *Zjawisko dezinformacji z perspektywy psychologicznej: uwarunkowania i przeciwdziałanie*, [in:] K. Stasiuk-Krajewska, M. Wenzel (eds.), *Dezinformacja w czasach kryzysu*, Wydawnictwo Adam Marszałek, Toruń 2024.

Marek M., *Operacja Ukraina – Kampanie dezinformacyjne, narracje, sposoby działania rosyjskich ośrodków propagandowych przeciwko państwu ukraińskiemu w okresie 2013–2019*, Wydawnictwo Difin SA, Warszawa 2020.

Miodek M. *(ed.), Dialog w Unii Europejskiej – scenariusze zajęć dydaktycznych z zakresu komunikacji, mediacji, stereotypów i przeciwdziałania dezinformacji,* Wydawnictwo Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2022.

Nowak T., *Działania hybrydowe w cyberprzestrzeni prowadzone przez Rosję jako zagrożenie dla bezpieczeństwa euroatlantyckiego*, [in:] M. Banasik, A. Rogozińska (eds.), *Zagrożenia Federacji Rosyjskiej i Bezpieczeństwo Międzynarodowe*, Wydawnictwo Difin SA, Warszawa 2020.

Nowak T., *Polityka Unii Europejskiej w latach 2014–2019 wobec działań hybrydowych Federacji Rosyjskiej*, [in:] M. Banasik, A. Rogozińska (eds.), *Zagrożenia Federacji Rosyjskiej i Bezpieczeństwo Międzynarodowe*, Wydawnictwo Difin SA, Warszawa 2020.

Proposal for a Regulation of the European Parliament and of the Council on ENISA, repealing Regulation (EU) No 526/2013, and on cybersecurity certification of information and communication technologies (OJ EU C 227/13 of 28.6.2018).

Rejman B., Rejman K., *Fake news jako narzędzie działań dezinformacyjnych a bezpieczeństwo współczesnych systemów społeczno–ekonomicznych*, [in:] K. Rejman, M. Wilczyńska, J. Wołejszo (eds.), *Bezpieczeństwo Informacji Wobec Współczesnych Zagrożeń*, Wydawnictwo Kaliskie Towarzystwo Przyjaciół Nauk, Kalisz 2023.

Stasiuk-Krajewska K., *Dezinformacja. Próba ujęcia dyskursywnego*, *Media – Kultura – Biznes*, Wydawnictwo Uniwersytet Gdański, Gdańsk 2023, vol. 1 (14).

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2020.

Szulc M., *Manipulowanie informacją w sieci za pomocą fake newsów jako zagrożenie dla młodzieży*, [in:] *Psychologia Wychowawcza*, Wydawnictwo Uniwersytet Gdański, Gdańsk 2020, vol. 599730, no. 17.

Tomaszewski S., *Media elektroniczne jako instrument walki informacyjnej*, [in:] W. Fehler (ed.), *Informacyjny Wymiar Bezpieczeństwa Państw i Jednostek*, Wydawnictwo Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2021.

Trish B., *Big Data under Obama and Trump: The Data-Fueled U.S. Presidency, Politics and Governance* (ISSN: 2183-2463), Cogitatio Press, Lisbon 2018.

Wisniewski B., Prońko J., *Ogniwa ochrony państwa*, Akademia Obrony Narodowej, Warszawa 2003.

Wiśniewski B., Sander G. S., *Zagrożenie, kryzys i sytuacji kryzysowa – jako uwarunkowania życia współczesnego człowieka*, "Bezpieczeństwo i Technika Pożarnicza", Nr 1/2016, Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej Państwowy Instytut Badawczy, Józefów 2016.

Wojnowski M., *Mit „wojny hybrydowej". Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku*, [in:] *Przegląd Bezpieczeństwa Wewnętrznego. Wojna hybrydowa – Wydanie Specjalne*, Wydawnictwo Agencji Bezpieczeństwa Wewnętrznego, Wiązowna 2015.

Wyzwania, szanse, zagrożenia i ryzyko dla bezpieczeństwa narodowego RP o charakterze wewnętrznym, R. Jakubczak, B Wiśniewski (red. nauk.), Wyższa Szkoła Policji w Szczytnie, Szczytno 2016.

About the Author

Marek Przybyła – his academic work focuses on issues of public security, the improvement of information security systems, and matters related to cybersecurity in the context of individuals and facilities of critical importance to the functioning of the state.

Marcin M. Brocki
WSB University in Dąbrowa Górnicza
e-mail: mbrocki94@gmail.com
ORCID: 0009-0002-0576-5224

DOI: 10.26410/SF_2/25/9

DIGITAL RISKS FOR CHILDREN AND ADOLESCENTS IN POLAND IN 2024 IN LIGHT OF THE 4 CS FRAMEWORK: AN ANALYSIS OF NATIONAL REPORTS

Abstract

The article analyses nationwide research from 2024 on the risks to which children and young people are exposed in the digital environment, using the 4C model. The study is based on reports entitled *Teenagers*, *Internet children*, and data from Dyżurnet.pl and the Office of the Ombudsman for Children's Rights. The results indicate that the 4C model can be used to classify threats and their nature, but it is difficult to create a matrix combining both approaches. The most common threats are harmful content, cyberbullying, and sexual threats, while there is a lack of data on commercial and contractual threats. The author emphasizes the need for in-depth research on child profiling, aggressive marketing, gambling mechanisms, as well as radicalization and more in-depth analysis of the risks associated with artificial intelligence.

Key words

digital safety, children and youth, 4C model, cyberbullying, harmful content

Introduction

The dynamically changing online environment creates a space for users in which development potential coexists with various forms of threats. Children and young people are a particularly vulnerable group, as their intense emotional and social development overlaps with their growing exposure to digital technologies. Although knowledge about the associated risks in Poland is steadily expanding, it remains scattered across many publications and reports, which creates a need to organize it.

The scale of the problem is illustrated by the results of nationwide surveys. The report *Internet dzieci* (Children and the Internet) notes that 85.6% of children aged 7–14 use the Internet, and in the 15–18 age group, this percentage is close to 100%[1]. In turn, the report *Nastolatki* (Teenagers) published by the Digital Citizenship Institute Foundation indicates that students in grades 7–8 of primary school and grades 1–2 of secondary school spend an average of 4 hours and 59 minutes in front of a screen on weekdays and 5 hours and 16 minutes on weekends. Most of them received their first smartphone at the age of 9–10, and about 40% before the age of 9[2].

It is worth noting that, unlike adults, adolescence is characterized by "multifaceted and intense changes" and tasks that "have a social dimension and are associated with gaining emotional independence"[3]. Early and frequent contact with the internet makes young users particularly vulnerable to threats that can disrupt this process, endanger their health and, in extreme cases, their lives. Such threats include misinformation, radicalization, cyberbullying, and exposure to age-inappropriate content.

These phenomena are also widely discussed in international literature. Research conducted by EU Kids Online, the International Telecommunication Union, and the Organization for Economic Co-operation and Development, among others, indicates that the internet is now one of the key environments in which young people operate. This requires systematic analysis of both the opportunities and threats associated with this ecosystem. Attention is drawn to the growing complexity of the digital environment, where risks arise not only from interpersonal relationships, but also from platform architecture, business models, and data processing methods.

Polish studies on the digital safety of children and young people emphasize that cyberspace is now an important area for socialization and relationship building. This is pointed out, among others, by B. Marciniec and D. Marczuk[4], who

1 M. Bigaj, K. Ciesiołkiewicz, K. Mikulski, A. Miotk, J. Przewłocka, M. Rosa, A. Załęska, *Internet dzieci. Raport z monitoringu obecności dzieci i młodzieży w internecie*, Warsaw 2025, p. 30.

2 A. Ładna, K. Kamiński, K. Rosłaniec, A. Wrońska, M. Błażej, A. Jankiewicz, F. Konopczyński, M. Nawrot, *Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców*, NASK – National Research Institute, Warsaw 2025, pp. 27–28.

3 A. I. Brzezińska, K. Appelt, B. Ziółkowska, *Psychologia rozwoju człowieka*, Sopot 2016, pp. 245–247.

4 B. Marciniec, D. Marczuk, "Bezpieczeństwo dzieci i młodzieży w przestrzeni wirtualnej", *Rozprawy społeczne* 2015, Vol. IX, No. 2, pp. 34–38.

highlight the growing importance of the online environment in the everyday lives of young people. A similar view is presented by J. Pyżalski[5], who shows that the online activity of adolescents (teenagers) combines both developmental and civic potential and various forms of risk.

Despite the growing number of national publications, their content often remains scattered and covers only selected aspects of risk. Some studies focus on legal issues[6], while others focus on the socialization and cultural dimensions[7]. However, there is still a lack of analyses that systematize threats in accordance with recognized international frameworks. Of particular importance here is the 4C classification (Content, Contact, Conduct, Contract) proposed by S. Livingstone and M. Stoilova[8], which provides a structured and comparable approach to the risks associated with children's use of the internet. This classification includes the following categories:

- Content – harmful material, e.g., pornography, harmful content, misinformation.
- Contact – the risk of contact with strangers online, e.g., grooming, phishing of minors, recruitment into criminal groups.
- Conduct – risks resulting from the actions of users themselves, e.g., cyberbullying, sharenting, doxing.
- Contract – threats resulting from the commercial exploitation of children, e.g., microtransactions, online gambling, advertising profiling of minors.

The authors also propose an additional dimension of classification, referring to the nature of the risk – aggressive, sexual, axiological, and commercial. However, the use of this perspective requires a detailed description and classification of threats, which is difficult due to the limited availability of data. In this context, there is a research gap regarding the lack of a synthetic analysis of Polish data in relation to the 4C model. Filling this gap would allow for a more precise assessment of the scale of individual types of risks and reliable comparisons with the results of international studies, in which this model is increasingly used.

The aim of this article is to organize knowledge about threats to children and young people on the Internet in 2024 by analyzing nationwide reports in relation to the 4C model. The article also aims to identify types of threats and areas requiring further research based on the results of the aforementioned summary in order to better understand the situation of young people in the digital world.

5 J. Pyżalski, "Positive Internet Use and Online Civic Engagement versus Active Involvement in Selected Online Risks – how are both connected in adolescents from six European countries?", *Psychology, Society & Education* 2023, Vol. XV, No. 3, pp. 16–17.

6 See: M. Olchanowski, "Bezpieczeństwo dzieci i młodzieży w cyberprzestrzeni…", *Zbliżenia Cywilizacyjne* 2017, Vol. XIII, No. 3, pp. 56–68.

7 See: M. Konopczyński, F. Konopczyński, "Młodzież, internet, socjalizacja…", in: A. Wrońska, R. Lew-Starowicz, A. Rywczyńska (eds.), *Edukacja – relacja – zabawa*, Warsaw 2019, pp. 21–25.

8 S. Livingstone, M. Stoilova, *The 4Cs: Classifying Online Risk to Children*, Hamburg 2021, p. 12.

Methodology

The study was based on a review of literature and reports addressing the threats faced by young people in Poland. The search included publications meeting the following criteria:

- The research was conducted in 2024 and was nationwide in scope.
- It concerned the issue of children and young people's exposure to risks associated with internet use.

On this basis, the following reports were selected for further analysis:

- Teenagers. Report from a nationwide survey of students and parents, published by NASK in 2025.
- Children's Internet. Report on monitoring the presence of children and young people on the Internet, published by the Digital Citizenship Institute Foundation in 2025.

The next step was to identify the behaviors and phenomena described in the reports that indicate the exposure of the surveyed children and young people to the risks of using the Internet, taking into account the scale of occurrence of these phenomena. The identified elements were then organized according to the 4C model concept.

The threats organized in this way made it possible to identify the categories of risks with which young people have the most frequent contact, as well as those that require greater attention due to the limited availability of empirical data.

The study was based largely on the use of theoretical methods, in particular: analysis – used to break down the issue into its constituent elements, including the identification and organization of threats found in the reports; synthesis – enabling the combination of the identified information and the assignment of the identified threats to the appropriate categories of the 4C model; abstraction – used to extract key elements from extensive research material; and generalization and inference, which allowed for the identification of the most important threats currently faced by children and young people, as well as the identification of areas requiring further empirical research due to the limited scope of available data[9].

Threats to children and young people online in Poland and the 4Cs concept

The Teenagers Report. a report from a nationwide survey of students and parents, published by NASK, focuses on how young people (students in grades 7–8 of primary school and grades 1–2 of secondary school) perceive and experience the digital world, especially the internet, and how parents assess their children's participation in the virtual space. Analysis of this document allows us to extract data relevant for further research:

9 See: J. Apanowicz, *Metodologia ogólna*, Gdynia 2002, pp. 23–28.

- 28% of teenagers declared that they had been victims of cybercrime, including:
  - account hacking – 12%,
  - theft of virtual goods – 8%,
  - hacking/data theft – 7%,
  - threats of violence in the real world – 6%,
  - blackmail/attempted extortion – 5%,
  - online shopping fraud – 5%,
  - impersonation/identity theft – 4%,
  - cryptocurrency fraud – 2%.
- Approximately 38–42% of respondents have experienced various forms of cyberbullying, including:
  - name-calling – 29%,
  - ridicule – 19%,
  - humiliation – 18%,
  - threatening – 13%,
  - blackmail – 13%,
  - disseminating compromising materials – 9%,
  - impersonating the subject – 8%.
- 22% of students declared that they had seen pathostreams at least once.
- 26% had participated in online challenges.
- 41% had encountered pornography; the average age of first contact was 11 years and 3 months.
- Sexting: 28% of students received nude or semi-nude photos from someone, and 5% sent such material themselves.
- Grooming: 11% of respondents had contact with adults they met online, of which 28% did not inform anyone about it.
- 67% of respondents declared that they had seen deepfake material at least once, i.e., material generated by artificial intelligence to mislead the recipient[10].

The report *Internet dzieci. Raport z monitoringu obecności dzieci i młodzieży w internecie* (Children on the Internet. Report on monitoring the presence of children and young people on the Internet), prepared by the Digital Citizenship Institute Foundation, presents the results of cross-media research recording actual Internet use on devices. Two age groups were distinguished: children (7–14 years old) and adolescents (15–18 years old). From the perspective of this article, the key data from the report include:

- 53.8% of adolescents (aged 15–18) and 51.3% of children (aged 7–14) have been exposed to pornography, with 25% of this group viewing such content at least once a month,

10 A. Ładna et al., *Nastolatki…*, op. cit., pp. 67, 69, 81, 85, 88, 92, 95, 101, 103, 137.

– 1.6 million children aged 7–12 use social media before reaching the age of 13, which represents over 66% of this population. It is worth noting that most social networking sites specify a minimum user age of 13 in their terms and conditions[11].

In the context of the nationwide survey conducted in 2024, it is worth mentioning two additional sources that broaden the perspective, although their full use in this analysis was difficult.

The first is the study Let's look at the internet through the eyes of children, commissioned by the Ombudsman. Respondents (aged 12-17) indicated that the most harmful threats in their opinion were: hate speech (84%), stalking (77%), and publishing someone's image without their consent (74%). These concerns partly overlap with the threats identified in the reports Teenagers and the Internet and Children and the Internet, concerning cyberbullying and sexting[12].

Another valuable source is the report on the activities of the Dyżurnet.pl team for 2024. It records the following incidents related to the sexual exploitation of minors:

– content depicting the sexual abuse of children – 11,147 incidents,
– content presenting children in a sexual context (e.g., modeling, posing) – 1,012 incidents,
– promotion of pedophilic activity – 29 incidents,
– child grooming – 26 incidents[13].

These data highlight the importance of research on sexual threats, especially in the context of pedophilia, grooming, and child pornography.

Table 1. Threats to children and young people from the perspective of the 4C concept

4C	Threat	Exposure of respondents to the threat expressed as a percentage.	Source
Content	Exposure to pornography	41% (primary school grades 7-8, secondary school grades 1-2), 53.8% (ages 15-18), 51.3% (ages 7-14)	Teenagers, Children's Internet
	Pathostreams	22%	Teenagers
	Participation in challenges	26%	Teenagers
	Social media <13 years old	over 66% (7-12 years old)	Children's internet use
	Deepfake	67%	Teenagers

11 M. Bigaj et al., *Internet dzieci…*, op. cit., pp. 41, 52–53.

12 Biuro Rzecznika Praw Dziecka, *Spójrzmy na internet oczami dzieci. Wyniki badań RPD*, Warsaw 2025.

13 Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy, *Raport 2024. Dyżurnet.pl*, Warsaw 2025, p. 18.

4C	Threat	Exposure of respondents to the threat expressed as a percentage.	Source
Contact	Grooming – contact with adults	11%	Teenagers
	Sexting – receiving sexual content	28%	Teenagers
	Threats of violence in real life	6%	Teenagers
Conduct	Name-calling	29%	Teenagers
	Ridicule	19%	Teenagers
	Humiliation	18%	Teenagers
	Threatening	13%	Teenagers
	Blackmailing	13%	Teenagers
	Compromising materials	9%	Teenagers
	Impersonation	8%	Teenagers
	Sexting – sending photos	5%	Teenagers
Contract	Account hacking	12%	Teenagers
	Theft of virtual goods	8%	Teenagers
	Hacking / data theft	7%	Teenagers
	Shopping fraud	5%	Teenagers
	Money extortion	5%	Teenagers
	Identity theft	4%	Teenagers
	Cryptocurrency fraud	2%	Teenagers

Source: own study.

A comparison of the reports on teenagers and the internet allows us to conclude that the Content category is the one with which children and young people in Poland have the most frequent contact (see Table 1). The most frequently mentioned threats are deepfakes, exposure to pornography, pathostreaming, and participation in online challenges. It is worth noting that not every challenge is negative (e.g., the second edition of the #Hot16Challenge in Poland), but the reports treat this phenomenon in a general way, which is due to the specific nature of the research.

An important category, although dominated by one phenomenon, is Conduct, in which cyberbullying remains the most common problem – almost every second student surveyed was a victim of it.

The Contact category, on the other hand, covers threats arising mainly from sexual relationships and contact with unknown adults.

The last category, Contract, was dominated by cybercrime phenomena, especially account and identity theft.

It is noteworthy that categories such as Contact, Contract, and Conduct turned out to be quite monothematic. This may indicate the need to consider a broader or more accurate spectrum of threats in future studies conducted by both the institutions indicated and independent researchers. This would provide a more complete picture of the threats faced by young Internet users.

The monothematic nature may also result from the general nature of the threats declared by participants, which makes it difficult to classify them according to the 4C model. The reports are dominated by references to cyberbullying, sexual threats, and cybercrime, while others, such as participation in challenges or deepfakes, remain too broadly described. Deepfakes appear in the report as a threat, but their nature has not been clearly defined, which further complicates their classification in the 4C model. This is also worth noting when analyzing deepfakes in the Teenagers report. Deepfake content encountered by respondents was most often used for jokes, ridicule, deception, and misinformation[14]. It is worth noting that this is the opinion of students on the use of this phenomenon, and not their actual exposure to this threat in this capacity. The current design of the study allows for a relatively precise identification of sexual and commercial threats, while it is more difficult to clearly classify those related to values and aggression so that they do not overlap between the 4C categories.

International reports mention other types of threats which, in the author's opinion, should be included in future Polish nationwide studies, e.g.:

Content:
- materials related to self-harm and suicide[15],
- violent content[16],
- extremist content[17],
- disinformation[18].

Contact:
- recruitment for criminal activities[19].

Conduct:
- doxxing[20].

14 A. Ładna et al., *Nastolatki…*, op. cit., p. 140.

15 D. Smahel, H. Machackova, G. Mascheroni et al., *EU Kids Online 2020: Survey Results from 19 Countries*, London 2020, pp. 61–62.

16 Office of Communications, *Children's Media Literacy Report 2024*, London 2024, pp. 23–24.

17 Ibid, p. 3.

18 Ibid, pp. 34–35.

19 European Union Agency for Law Enforcement Cooperation, *The Recruitment of Young Perpetrators for Criminal Networks*, The Hague 2024, pp. 2–3.

20 D. Smahel et al., *EU Kids Online 2020…*, op. cit., pp. 70–72.

Contract:
- loot boxes and other gambling-like mechanics[21],
- aggressive, hidden marketing aimed at children[22],
- profiling of children[23].

These are examples of threats that have been identified both in Poland and internationally. Many of them are changing rapidly and overlap between categories, which indicates the need for systematic monitoring. This list is not exhaustive – it is a proposal for further research.

Summary

The aim of this article was to organize knowledge about the threats described in nationwide reports on children and young people on the Internet in 2024 by analyzing them in relation to the 4C model and, based on the data obtained, to indicate possible directions for further research. Extending the analysis to include earlier studies and regional reports could enable a more comprehensive understanding of the phenomenon, observation of trends, and, in the longer term, the proposal of an original classification of threats based on the 4C model adapted to the Polish reality.

The risks described in the reports can be assigned to the 4C model based on the risk categories "Content, Contact, Conduct, and Contract." This allows us to conclude that the risks faced by young people are diverse. a nationwide study conducted in 2024 analyzed the exposure of children and young people to a number of risky phenomena encountered by a large proportion of young respondents. However, it is worth noting a certain concentration around the risks studied – issues related to cyberbullying, harmful content, and sexual threats dominated among them.

The greatest data deficiency is visible in the Contract category, where reports focused mainly on cybercrime issues. Future studies should also analyze phenomena such as the use of so-called loot boxes or other gambling-like mechanisms, as well as the problem of profiling children on the internet and their exposure to aggressive marketing. The rapidly developing threats associated with artificial intelligence should also be taken into account. The reports address both this issue and the way in which children and young people use these technologies. In the context of threats, it was mainly considered as deepfake, which is a very accurate perception of the problem. At the same time, it is worth considering the nature of such content in the context of deepfakes, e.g., radicalizing, pornographic, disinformation, inciting violence. With the development of this technology, it is also worth monitoring new threats that may emerge in connection with the development of language models and other AI-based tools.

21 Organisation for Economic Co-operation and Development, *Consumer Vulnerability in the Digital Age*, Paris 2023, pp. 20–21.

22 Ibid, pp. 36–38.

23 Ibid, pp. 24–26.

It is worth noting that the classification of threats according to their nature (e.g., aggressive, sexual, axiological, commercial) is currently difficult due to the limited level of detail of the available data. With the current state of knowledge, it is possible to classify threats according to the 4C model types, but creating a complete, non-duplicative matrix of threat categories and nature would require more precise data. Obtaining such data may be challenging, among other things due to the fact that the respondents in these studies are minors.

Nevertheless, in the author's opinion, such an effort is necessary. It would allow for a more detailed understanding of the nature of the risks faced by children and young people in the digital environment and for the development of a coherent research framework adapted to the specificities of the Polish social context.

Bibliography

Apanowicz J., Metodologia ogólna, Gdynia 2002.

Bigaj M., Ciesiołkiewicz K., Mikulski K., Miotk A., Przewłocka J., Rosa M., Załęska A., Internet dzieci. Raport z monitoringu obecności dzieci i młodzieży w internecie, Warszawa 2025.

Biuro Rzecznika Praw Dziecka, Spójrzmy na internet oczami dzieci. Wyniki badań RPD, Warszawa 2025.

Brzezińska A. I., Appelt K., Ziółkowska B., Psychologia rozwoju człowieka, Sopot 2016.

European Union Agency for Law Enforcement Cooperation, The Recruitment of Young Perpetrators for Criminal Networks, The Hague 2024.

Smahel D., Machackova H., Mascheroni G., Dedkova L., Staksrud E., Ólafsson K., Livingstone S., Hasebrink U., EU Kids Online 2020: Survey Results from 19 Countries, London 2020.

Konopczyński M., Konopczyński F., „Młodzież, internet, socjalizacja – w perspektywie współczesnych paradygmatów społecznych", w: A. Wrońska, R. Lew-Starowicz, A. Rywczyńska (red.), Edukacja – relacja – zabawa. Wieloaspektowość internetu w wymiarze bezpieczeństwa dzieci i młodzieży, s. 14–39, Warszawa 2019.

Livingstone S., Stoilova M., The 4Cs: Classifying Online Risk to Children, Hamburg 2021.

Ładna A., Kamiński K., Rosłaniec K., Wrońska A., Błażej M., Jankiewicz A., Konopczyński F., Nawrot M., Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców, NASK – Państwowy Instytut Badawczy, Warszawa 2025.

Marciniec B., Marczuk D., „Bezpieczeństwo dzieci i młodzieży w przestrzeni wirtualnej", Rozprawy społeczne, t. IX, nr 2, 2015, s. 34–38.

Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy, Raport 2024. Dyżurnet.pl, Warszawa 2025.

Office of Communications, Children's Media Literacy Report 2024, London 2024.

Organisation for Economic Co-operation and Development, Consumer Vulnerability in the Digital Age, Paris 2023.

Olchanowski M., „Bezpieczeństwo dzieci i młodzieży w cyberprzestrzeni na podstawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej na lata 2017–2022", Zbliżenia Cywilizacyjne, t. XIII, nr 3, 2017, s. 56–69.

Pyżalski J., „Positive Internet Use and Online Civic Engagement versus Active Involvement in Selected Online Risks – how are both connected in adolescents from six European countries?", Psychology, Society & Education, t. XV, nr 3, 2023, s. 10–18.

Telemedia Management GmbH, Safeguarding Children Online: a Service-Specific View on Risks and Parental Attitudes, Geneva 2023.

About the Author

Marcin Brocki is a doctoral researcher in security studies at the WSB Academy, whose research interests national and human security, safety education, and youth cybersecurity. His academic background is complemented by practical experience within crisis-management structures, including work at the Emergency Notification Center, as well as by teaching activity in the fields of security and civic education.

Małgorzata Terlecka-Maciejewska, PhD
Voivodeship Combined Hospital in Skierniewice
e-mail: lek.mterlecka@gmail.com
ORCID: 0009-0009-7589-9237

DOI: 10.26410/SF_2/25/10

LEGAL STATUS OF PREPARATIONS BY INDEPENDENT PUBLIC HEALTHCARE INSTITUTIONS FOR NATIONAL DEFENSE NEEDS

Abstract

The Regulation of the Council of Ministers of October 27, 2023, *on the preparation and use of medical entities for national defense purposes*, which replaced the Regulation of the Council of Ministers of June 27, 2012, *on the conditions and methods of preparation and use of medical entities for national defense purposes and the jurisdiction of authorities in these matters*, organizes the existing legal framework regarding the preparation of medical entities to operate in the event of an external threat to national security and during wartime. It creates a foundation for planning and implementing tasks while taking into account the responsibilities and hierarchical competencies of public administration authorities. The regulation identifies the authorities responsible for organizing, imposing, supervising, and controlling the tasks carried out for national defense purposes, which serves as the starting point for organizing the entire defense preparation process involving medical entities. The substantive provisions contained in the regulation are largely similar to those from the 2012 regulation. However, an additional area covered by the new legal act includes defense preparations carried out by operators of emergency medical teams, including air ambulance teams.

Keywords

law, defense preparations, defense needs, medical entity

Introduction

For centuries, the security of the state was equated with freedom from military threats. Over time, however, other dimensions of threats were recognized and identified, beyond the mere danger of armed attack. It was established that protection against external aggression is only one of many challenges that must be addressed in order to ensure state security, whose contemporary scope also includes, among others, economic, environmental, social, and health-related aspects.[1]

In the context of contemporary challenges related to national security, the role of healthcare institutions within the state's defense system is becoming increasingly important. Changing geopolitical conditions, climate change, as well as threats related to epidemics and other humanitarian crises, require the healthcare sector not only to maintain the ability to respond under normal circumstances, but also to prepare for extraordinary situations. In the face of such threats, legal regulations form the foundation for the operation of healthcare institutions, defining their obligations in support of national defense.

Understanding the legal aspects of the preparedness of healthcare institutions for the state's defense needs is crucial not only for the medical institutions themselves, but also for decision-makers and society as a whole, which must be aware that in the event of an external threat to national security or during wartime, healthcare institutions will be required to undertake a tremendous effort to ensure the provision of medical services, both to those injured as a result of military actions and to the civilian population who, though not directly affected by the ongoing conflict, will nevertheless require healthcare.[2]

The evolution of legal regulations in the area of defense preparedness of healthcare institutions

The legal act regulating the area of defense preparedness of healthcare institutions, as part of the non-military component of the state's defense system, is the Regulation of the Council of Ministers of October 27, 2023, *on the preparation and use of healthcare institutions for the state's defense needs*, which was amended by the Regulation of the Council of Ministers of September 25, 2024, *amending the regulation on the preparation and use of healthcare institutions for the state's defense needs*[3]. The regulation defines the conditions and the manner of preparation and use of healthcare

1 See.: W. Kitler, *Obrona narodowa w wybranych państwach demokratycznych*, Warsaw 2001, W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, Warsaw 2011, A. Czupryński, B. Wiśniewski, J. Zboina (red. nauk.), *Nauki o bezpieczeństwie. Wybrane problemy badań*, Józefów 2017, G. Gielerak, *System ochrony zdrowia na miarę potrzeb oraz współczesnych wyzwań i zagrożeń*, „Menedżer Zdrowia" 2022, No. 5-6, M. Kuliczkowski, L. Sawicki, *Pozamilitarne przygotowania obronne w Polsce*, Warsaw 2020.

2 Terlecka-Maciejewska M., Wywiał P., *Improving the preparedness of independent public healthcare institutions for national defense needs in the area of operational organization*, „Security Forum" 2025, Volume 9, No 1, p. 99-114.

3 Regulation of the Council of Ministers of September 25, 2024, *amending the regulation on the preparation and use of healthcare institutions for the state's defense needs* (Journal of Laws, item 1456).

institutions, as understood under the Act of April 15, 2011 on Medical Activity, for the state's defense needs. The conditions of implementation constitute a set of factors and requirements that determine the way in which a given undertaking is carried out. They cover various aspects related to the execution of the task, such as organizational and procedural requirements or the deadline for completion. Properly defining the conditions of implementation is essential for the entity responsible for carrying out the undertaking, as it allows for a clear specification of expectations, which contributes to the smooth and effective execution of tasks. The manner of implementation, in turn, refers to the methods, techniques, and procedures applied to accomplish a specific task and encompasses all actions necessary to achieve the intended goals and outcomes. In practice, the manner of implementation may include elements such as planning, resources, control, and evaluation. Therefore, the manner of implementation is crucial for the success of any undertaking, as it directly affects efficiency and the ability to achieve the expected results.

The entry into force of the 2023 regulation resulted in the repeal[4] of the Regulation of the Council of Ministers of June 27, 2012, *on the conditions and manner of preparation and use of healthcare institutions for the state's defense needs and the competence of authorities in these matters*[5], issued on the basis of the repealed Act of November 21, 1967, on the Universal Obligation to Defend the Republic of Poland. The regulation "organizes the existing legal framework regarding the preparedness of healthcare institutions to operate in the event of an external threat to the state's security and during wartime, creating a foundation for planning and implementing tasks while taking into account the responsibilities and hierarchical competences of public administration authorities. The introduced changes are the result of many years of experience of public administration bodies and healthcare institutions in this area, and are intended to improve the planning and implementation of undertakings carried out for the state's defense needs with the participation of healthcare institutions."[6]

The first legal act that defined the conditions and manner of preparation and use of the healthcare system for the state's defense needs was the Regulation of the Council of Ministers of May 18, 2004, *on the conditions and manner of preparation and use of public and non-public healthcare services for the state's defense needs, as well as the competence of authorities in these matters*[7]. In the context of this study, particular attention should be paid to the provisions concerning outpatient care and ambulatory healthcare services. The conditions and manner of preparing the

4 Act of March 11, 2022 on the Defense of the Fatherland (Journal of Laws of 2025, item 825), Article 821(1).

5 Regulation of the Council of Ministers of June 27, 2012 *on the conditions and manner of preparation and use of healthcare institutions for the state's defense needs and the competence of authorities in these matters* (Journal of Laws, item 741).

6 Justification to the draft of October 2, 2023 of the Regulation of the Council of Ministers of … 2023 *on the preparation and use of healthcare institutions for the state's defense needs*, p. 25.

7 Regulation of the Council of Ministers of May 18, 2004, *on the conditions and manner of preparation and use of public and non-public healthcare services for the state's defense needs, as well as the competence of authorities in these matters* (Journal of Laws No. 143, item 1515).

healthcare system for the state's defense needs, as set out in the original 2004 regulation, concerned, among other things, the planning and implementation of tasks related to determining minimum staffing standards and employment indicators in healthcare facilities, as well as the operation of outpatient care. Furthermore, it was emphasized that "ambulatory healthcare for the state's defense needs is maintained to the same extent and scope as during peacetime."[8] At the same time, it was indicated that necessary transfers of medical personnel to healthcare facilities forming the hospital base are carried out based on the provincial plan for medical personnel transfers. It should be noted that the regulation provided for the maintenance of abbreviated medical documentation in the event of mass sanitary casualties to ensure proper classification of the wounded and sick, maintain continuity of medical and evacuation care, and implement the marking of the wounded and sick by means of the classification signs specified in the annex to the regulation. The annexes also specified the "Indicators and standards for employment of medical staff in healthcare facilities in situations of threat to state security and wartime," divided into hospitals, auxiliary hospital facilities, regional blood donation and transfusion centers, as well as a template for the "Report on the transfer of wounded and sick persons in healthcare organizational units."

In 2009, by virtue of the Regulation of the Council of Ministers[9] amending the regulation under analysis, the planning and implementation of tasks concerning the operation of outpatient care were replaced with "ambulatory healthcare activities."[10] At the same time, definitions were introduced for "ambulatory healthcare" and "organizational unit of the public healthcare system." Ambulatory healthcare was understood as "the provision of healthcare services by providers to persons not requiring treatment in round-the-clock or full-day conditions."[11] From the organizational units of the public healthcare system, constituting healthcare facilities under the Act of August 30, 1991 on Healthcare Facilities, certain institutions were excluded from the obligation to prepare for defense needs based on the provisions of the regulation. These exclusions included healthcare facilities established by the Minister of National Defense, outpatient clinics or outpatient clinics with inpatient wards of the Police, the State Fire Service, the then Government Protection Bureau, the Internal Security Agency, as well as public healthcare facilities of the Border Guard and healthcare facilities for persons deprived of liberty.[12]

The 2009 Regulation of the Council of Ministers represented an important step toward improving and standardizing defense preparedness in the healthcare sector, ensuring better readiness of healthcare institutions to operate in conditions of

8 Ibidem, § 11(1).

9 Regulation of the Council of Ministers of November 3, 2009, *amending the regulation on the conditions and manner of preparation and use of public and non-public healthcare services for the state's defense needs and the competence of authorities in these matters* (Journal of Laws No. 202, item 1555).

10 Ibid., § 1(1)(a).

11 Ibidem, point 2.

12 Ibidem.

external threats to the state's security and during wartime. This was achieved by clarifying the competences of authorities responsible for defense preparedness in the healthcare sector and by providing detailed regulations on planning matters. The introduced changes contributed to better integration of healthcare institutions' defense preparations with the overall system of national defense preparedness.

The entry into force of the Regulation of the Council of Ministers of June 27, 2012, repealed the provisions of the 2004 and 2009 regulations. In terms of the conditions and manner of preparation and use of healthcare institutions for the state's defense needs, the planning and implementation of tasks included the provision of ambulatory healthcare services as well as the determination of staffing requirements and employment indicators in healthcare institutions.[13] Similarly to the solutions contained in the 2009 regulation, healthcare institutions subordinate to or supervised by the Minister of National Defense, the minister responsible for internal affairs[14], the Minister of Justice, and the Head of the Internal Security Agency–possessing a hospital, outpatient clinic, outpatient clinic with inpatient wards, or a primary healthcare physician in their organizational structure–were exempted from the obligation to prepare for the state's defense needs under the provisions of the new regulation. Furthermore, the regulation contained a provision analogous to that of the 2009 regulation regarding the role of ambulatory healthcare services, stating that "ambulatory healthcare services for the state's defense needs are provided to the same extent as during peacetime,"[15] and that necessary transfers of medical personnel to healthcare institutions forming the hospital base are carried out based on the needs identified in the prepared medical personnel balances and personnel transfer plans. Additionally, the annexes to the regulation specified, among other things, the "Employment indicators for medical personnel" and the "Method of allocating hospital beds for uniformed services by healthcare institutions performing defense tasks and the coordination of authorities in this regard."

Current state of legal and organizational solutions

The substantive regulations in the Regulation of October 27, 2023, are similar to those in the earlier regulation of June 2012. An additional area, not covered by the previous regulations, concerns defense-related preparations carried out by operators of medical rescue teams, including air rescue teams. The regulation specifies the conditions and manner of performing tasks for the state's defense needs by certain groups of healthcare institutions, while simultaneously indicating the scope of the activities to be carried out by them:

13 Regulation of the Council of Ministers of June 27, 2012, *on the conditions and manner…*, § 1(1)(1)(c–d).

14 However, the exemption does not apply to organizational units of the public blood service and units responsible for sanitary and epidemiological protection that are subordinate to or supervised by the Minister of National Defense and the competent minister.

15 Regulation of the Council of Ministers of June 27, 2012, *on the conditions and manner…*, § 14(1).

- hospitals (and other healthcare facilities, if necessary) are obliged to prepare for an increased provision of hospital services, including for the needs of uniformed services, by planning an appropriate number of hospital beds;
- operators of medical rescue teams are required to prepare for an increased provision of healthcare services by medical rescue teams;
- healthcare institutions designated for coordination and planning the provision of healthcare services in substitute hospital facilities;
- regional blood donation and transfusion centers are obliged to prepare to ensure the supply of blood, its components, and blood-derived products;
- sanitary and epidemiological stations are required to prepare to ensure sanitary and epidemiological protection, planning an increase in readiness and capacity for this purpose.

The conditions and manner of preparation and use of healthcare institutions for the state's defense needs cover three areas: the planning and implementation of tasks, the coordination, and the cooperation of public administration authorities, healthcare institutions, and other organizational units in the planning and execution of these tasks.[16] Accordingly, the planning and implementation of tasks takes place in the following areas:

- provision of hospital services, including for the needs of uniformed services;
- provision of healthcare services in substitute hospital facilities;
- provision of healthcare services for the national security management system;
- provision of healthcare services by medical rescue teams and air medical rescue teams;
- ensuring the supply of blood, its components, and blood-derived products;
- ensuring sanitary and epidemiological protection.

In the process of planning the above-mentioned activities, the implementation of the following tasks is taken into account:[17]

- ensuring the necessary personnel, in particular medical personnel;
- ensuring the necessary support in terms of infrastructure, services, procedures, equipment, and supplies;
- organizing defense trainings;
- exempting individuals from the obligation to perform active military service in the event of mobilization or during wartime;
- providing material and personal services;
- carrying out other activities necessary for the preparation and use of healthcare institutions for the state's defense needs.

According to the adopted assumptions, the regulation indicates the authorities competent to organize, impose, supervise, and control tasks carried out for the state's defense needs, which constitutes the starting point for organizing the entire

16 Regulation of the Council of Ministers of October 27, 2023, *on the preparation and use of healthcare institutions…*, § 4(1)(1).

17 Ibidem, § 4(2).

defense preparedness process involving healthcare institutions. Considering the fact that healthcare institutions established by the minister responsible for internal affairs, the Minister of Justice, the Minister of National Defense, or the Head of the Internal Security Agency are units subordinate to or supervised by these authorities, the performance of defense tasks by these institutions is conducted within the framework of the operational planning process carried out by these authorities. At the same time, it should be noted that defense tasks can be classified as statutory tasks of these healthcare institutions, and the scope of their potential use is limited exclusively to the needs of the relevant authority, as determined by internal regulations. Therefore, the provisions of the regulation do not apply to the aforementioned healthcare institutions. However, the exemption from the above limitation for certain tasks of healthcare institutions established by the Minister of National Defense refers to tasks related to coordinating or supervising the activities of other authorities or healthcare institutions.[18]

The authorities competent to organize, impose, control, and supervise tasks related to the planning and implementation of activities in the provision of hospital services, including for the needs of uniformed services, the provision of healthcare services in substitute hospital facilities, and for the national security management system are the voivode and the commune head, mayor, city president, county head, or the marshal of the voivodeship. The voivode territorially competent for the place of task implementation is the authority responsible with respect to local government units, healthcare institutions that are independent public healthcare facilities or budgetary units for which the founding entity is different from a local government unit, in agreement with that founding entity, as well as other healthcare institutions not mentioned above. With regard to local government units, the voivode is the competent authority for tasks carried out by these units and tasks carried out by healthcare institutions that are independent public healthcare facilities or budgetary units for which the founding entity is the given local government unit, as well as for healthcare institutions established as capital companies in which the local government unit holds at least 51% of shares or stock. Local government authorities, in turn, are competent with respect to independent public healthcare facilities or budgetary units.

The authorities competent to organize, impose, control, and supervise tasks related to the planning and implementation of activities in the provision of healthcare services by medical rescue teams and air medical rescue teams are, respectively, the voivode – with regard to healthcare institutions operating medical rescue teams – and the minister responsible for health – with regard to the healthcare institution operating air medical rescue teams. The minister responsible for health is also the competent authority for tasks related to ensuring the supply of blood, its components, and blood-derived products. However, the minister exercises his authority in organizing, controlling, and supervising these tasks through the National Blood Center.

18 Justification to the draft of October 2, 2023 of the Regulation of the Council of Ministers…., p. 25-26.

The authorities competent to organize, impose, control, and supervise tasks related to sanitary and epidemiological protection are the voivode and the Chief Sanitary Inspector, respectively with regard to territorially competent provincial, district, and border sanitary and epidemiological stations.

The imposition of tasks concerning the planning and implementation of activities for the state's defense needs by competent authorities is carried out by administrative decision, ordinance, or order of the competent authority. The imposition of tasks by administrative decision applies to tasks assigned to healthcare institutions that are independent public healthcare facilities or budgetary units for which the founding entity is different from a local government unit, as well as to other healthcare institutions, excluding independent public healthcare facilities and certain budgetary units.

Tasks are imposed by ordinance by the voivode – with respect to tasks assigned by him to local government units – and by competent authorities in cases other than those specified above. In cases other than those specified above, competent authorities may also impose tasks related to the planning and implementation of activities for the state's defense needs in the form of an order.

It should be noted that tasks concerning the planning and implementation of activities in the provision of hospital services and healthcare services, as well as in ensuring the supply of blood, its components, and blood-derived products, and sanitary and epidemiological protection, imposed by competent authorities on healthcare institutions and local government units, should be consistent with the tasks imposed on these entities within the framework of the operational planning process. Synchronization of activities in this regard is ensured through the cooperation of competent authorities.

When addressing the conditions and manner of preparation and use of healthcare institutions for the state's defense needs, attention should also be paid to the role and position of the so-called departmental representative[19]. The departmental representative is a person designated to cooperate with the voivode and the heads of healthcare institutions in planning and implementing tasks related to the provision of hospital services for the needs of uniformed services and healthcare services for the national security management system. In addition, they are responsible for the storage of equipment and individual weapons of soldiers and officers admitted for treatment and rehabilitation in healthcare institutions. In consultation with the competent authorities, they also supervise the provision of the above mentioned hospital and healthcare services and the referral of soldiers and officers completing treatment to departmental medical commissions.

It should also be noted that for each military medical support region – i.e., a designated area of the country encompassing the administrative territory of one or

19 A departmental representative is a person designated by the Minister of National Defense, the minister responsible for internal affairs, the Head of the Internal Security Agency, or the Head of the Intelligence Agency, authorized to represent that authority in matters concerning the provision of hospital services for the needs of uniformed services and healthcare services for the national security management system (source: Regulation of the Council of Ministers of September 25, 2024, *amending the regulation on preparation…*, § 1(1)).

more voivodeships, within which healthcare institutions' tasks for the state's defense needs are organized and implemented – a leading healthcare institution has been appointed and established by the Minister of National Defense, whose commander also serves as the commander of the military medical support region. Eight military medical support regions have been designated, along with the identification of the leading healthcare institution and the assignment of the area of responsibility.

Summary

In summary, unlike the provisions contained both in the Regulation of the Council of Ministers of May 18, 2004, and in the Regulation of the Council of Ministers of June 27, 2012, *on the conditions and manner of preparation and use of healthcare institutions for the state's defense needs and the competence of authorities in these matters*, the Regulation of the Council of Ministers of October 27, 2023, *on the preparation and use of healthcare institutions for the state's defense needs* does not mention the provision of ambulatory healthcare services in the area of planning and implementing tasks for defense purposes, nor does it specify their scope. Furthermore, when defining the conditions and manner of performing tasks for defense purposes by specific groups of healthcare institutions, while simultaneously indicating the scope of activities to be carried out, independent public healthcare facilities were not included. Healthcare institutions that do not participate in the implementation of the tasks specified in the regulation for the state's defense needs, or participate in such tasks only within a limited scope of their operations, are required, in the event of an external threat to the state's security and during wartime, to provide healthcare services as far as possible in the same manner as during peacetime. At the same time, the regulation anticipates a limitation of the activities of such an institution if its medical personnel, infrastructure, equipment, or supplies are allocated for use in tasks carried out for the state's defense needs.[20]

Based on the conducted scientific research, it can therefore be concluded that independent public healthcare facilities providing healthcare services on an outpatient basis, if assigned defense tasks specified by the regulation, will primarily participate in the planning and implementation of tasks related to the provision of healthcare services for the national security management system and in substitute hospital facilities. Furthermore, outpatient healthcare services for the state's defense needs will be provided to the same extent as during peacetime, differing only in terms of dynamics and intensity. Despite the exemption of employees from the obligation to perform military service, any potential transfers of medical personnel from independent public healthcare facilities to healthcare institutions forming the hospital base will be carried out based on the needs identified in the medical personnel balances prepared according to the current operational situation.

20 Regulation of the Council of Ministers of October 27, 2023, *on the preparation and use of healthcare institutions…*, § 19.

Bibliography

Act of March 11, 2022 on the Defense of the Fatherland (Journal of Laws of 2025, item 825).

Justification to the draft of October 2, 2023 of the Regulation of the Council of Ministers of … 2023 *on the preparation and use of healthcare institutions for the state's defense needs.*

Czupryński A., Wiśniewski B., Zboina J. (red. nauk.), *Nauki o bezpieczeństwie. Wybrane problemy badań*, Józefów 2017.

Gielerak G., *System ochrony zdrowia na miarę potrzeb oraz współczesnych wyzwań i zagrożeń*, „Menedżer Zdrowia" 2022, p. 5-6.

Justification to the draft of October 2, 2023 of the Regulation of the Council of Ministers of … 2023 *on the preparation and use of healthcare institutions for the state's defense needs.*

Kitler W., *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, Warsaw 2011.

Kitler W., *Obrona narodowa w wybranych państwach demokratycznych*, Warsaw 2001.

Kuliczkowski M., Sawicki L., *Pozamilitarne przygotowania obronne w Polsce*, Warsaw 2020.

Regulation of the Council of Ministers of June 27, 2012 *on the conditions and manner of preparation and use of healthcare institutions for the state's defense needs and the competence of authorities in these matters* (Journal of Laws, item 741).

Regulation of the Council of Ministers of May 18, 2004, *on the conditions and manner of preparation and use of public and non-public healthcare services for the state's defense needs, as well as the competence of authorities in these matters* (Journal of Laws No. 143, item 1515).

Regulation of the Council of Ministers of November 3, 2009, *amending the regulation on the conditions and manner of preparation and use of public and non-public healthcare services for the state's defense needs and the competence of authorities in these matters* (Journal of Laws No. 202, item 1555).

Regulation of the Council of Ministers of September 25, 2024, *amending the regulation on the preparation and use of healthcare institutions for the state's defense needs* (Journal of Laws, item 1456).

Terlecka-Maciejewska M., Wywiał P., *Improving the preparedness of independent public healthcare institutions for national defense needs in the area of operational organization*, „Security Forum" 2025, Volume 9, No. 1, p. 99-114.

About the Author

Małgorzata Terlecka-Maciejewska – Deputy Director for Healthcare at the Voivodeship Combined Hospital in Skierniewice, a specialist in ophthalmology. She holds a PhD in social sciences in the field of security studies. Her work focuses on healthcare management, with particular emphasis on the operational safety of medical entities in crisis situations. She is the author of scientific publications that combine medical knowledge with management practice and risk analysis in the healthcare system.

Albert Kościński, M. Sc.
WSB University in Dąbrowa Górnicza
e-mail: albert.koscinski@gmail.com
ORCID: 0009-0003-6986-4878

DOI: 10.26410/SF_2/25/11

SAFETY OF RESCUERS DURING AVALANCHE OPERATIONS

Abstract

The aim of this article is to analyze how the level of training of mountain rescue personnel affects their safety during avalanche rescue operations. The study was based on a survey conducted among members of the Polish Mountain Rescue Service (GOPR), completed by 36 respondents with various levels of experience. The author hypothesized that a higher level of training is linked to a higher level of safety during rescue missions. The article discusses how avalanches form, the main factors that trigger them, key aspects of rescue operation planning, and the importance of modern rescue equipment used in avalanche terrain. The results clearly show that mountain rescuers are aware of both terrain and weather-related risks. They recognize the importance of good organization, familiarity with rescue gear, and working in well-coordinated teams. Most respondents take part in avalanche training regularly, which improves their confidence and readiness for real missions. The findings support the hypothesis: regular training, field experience, and proper use of rescue equipment are essential for ensuring the safety of mountain rescuers working in avalanche-prone areas.

Keywords

mountain rescue, avalanche, safety

Introduction

An avalanche is a rapid, spontaneous movement of snow masses down a mountain slope, representing one of the most serious natural hazards in high-mountain areas. The mechanism of its formation is complex and results from the interaction of three main factors: snow, terrain shape, and atmospheric conditions[1].

The stability of the snow cover depends on its internal structure–especially the type, hardness, moisture, and layering of the snow[2]. The heterogeneity of this structure, caused by snow metamorphism and external factors (e.g., precipitation, wind, temperature fluctuations), leads to the formation of layers with varying cohesion and strength[3]. In particular, weakly bonded layers to the substrate form potential sliding planes for the upper snow layers. Among the terrain factors favoring avalanches, slope angle is the most important–the greatest risk occurs on slopes with an inclination of 30–45 degrees[4]. Geographic orientation and wind exposure are also significant, influencing the distribution and characteristics of snow deposits.

Meteorological conditions, such as heavy snowfall or rain, sudden temperature changes, and solar radiation, can disrupt the balance of the snow cover by increasing its mass, changing the physicochemical properties of the snow, or creating wet layers[5]. Human activity also plays an important role–over 90% of avalanches involving people are directly triggered by them[6].

Understanding the mechanisms leading to snow cover destabilization is crucial for avalanche risk assessment and effective safety management in mountainous areas.

Snow avalanches pose a serious threat to people in mountain regions. Statistics show an increase in avalanche incidents worldwide, linked to the changing climate of our planet, including global warming[7].

Increased interest in winter tourism and a growing number of people actively spending time in the mountains during winter mean that a larger number of potential victims may be present in avalanche-prone areas. As a consequence of these two factors, the number of avalanche accidents requiring organized rescue operations may consistently increase year by year.

Every avalanche accident poses a serious threat to the life and health of people within the danger zone, including rescuers[8]. Rescue operations in avalanche areas are

1 A. O'Baron, M. Clelland, *a Guide To Staying Safe In Avalanche Terrain*, 2012, p 1-5.

2 T. Kurzeder, H. Feist, *Lawinen. Risiko-Check fur Freerider*, Insbruck 2012, p. 58-65.

3 M. Kacperek, *Kochaj śnieg – unikaj lawin*, Kraków 2004, p. 38-43.

4 T. Kurzeder, H. Feist, *Lawinen. Risiko-Check fur Freerider*, Insbruck 2012, p. 17.

5 A. O'Baron, M. Clelland, *a Guide To Staying Safe In Avalanche Terrain*, 2012, p 52-58.

6 M. Kacperek, *Kochaj śnieg – unikaj lawin*, Kraków 2004, s. 20, p. 74-79.

7 J. A. Ballesteros-Cánovas et al., *Climate warming enhances snow avalanche risk in the Western Himalayas*, PNAS 2018; B. Berwyn, *How Climate Change May Influence Deadly Avalanches*, SCIAM 2021; H. Nabi, *How climate change worsens avalanches in the Himalayas,* Dialogue Earth 2023.

8 W. Andrusikiewicz , *Ratownictwo górskie w kontekście narażenia zawodowego*, conference materials, AGH 2023.

extremely risky and require specialized skills and proper preparation to minimize risks for those involved[9]. Currently, due to growing winter tourism and sports activity as well as increased avalanche risk, there is a need to assess safety and adequately prepare rescuers for operations in avalanche zones[10].

The issue of rescuer safety in avalanche terrain has always been a matter of balancing the shortest possible exposure time of rescuers in the avalanche area with conducting a thorough enough search to locate all buried victims[11]. In 2019, Albert Lunde and Christen Tellefsen conducted a retrospective study of avalanche accidents in Norway from 1996 to 2017, resulting in recommendations for the deployment and prioritization of rescue forces and resources at avalanche sites, taking into account the safety of both victims and rescuers on site[12]. The main conclusion of this study was that patients should receive appropriate treatment at the right place and time, and that the allocation of rescue resources should aim to reduce the time rescuers spend in avalanche terrain, especially in cases without confirmed victims.

Methodology

The aim of this article is to answer the research question: How do the experience and training level of mountain rescuers influence their awareness of hazards and their safety during rescue operations in avalanche terrain?

The author of this article formulates the following hypothesis: as the training level of mountain rescuers in avalanche rescue increases, their safety during rescue operations in avalanche terrain also improves.

The article also presents the main factors determining risks for rescuers, as well as safety strategies that can be applied to minimize dangers associated with rescue operations in avalanche areas. This analysis allows for a better understanding of safety requirements for rescuers and the identification of areas needing further research and the development of rescue practices.

A high level of training in avalanche rescue contributes to rescuers' skills and competencies in identifying and responding to hazards encountered during rescue operations in avalanche terrain. Experienced rescuers are better equipped to plan rescue actions, make appropriate decisions, and coordinate activities under difficult conditions in avalanche areas. Correct and proficient use of specialized rescue equipment can increase the efficiency of rescue operations by minimizing the time needed to locate and save buried victims, thereby reducing rescuers' exposure to danger while operating in avalanche terrain. High-quality training and regular skill

9 C. Van Tilburg et al., *Wilderness Medical Society Clinical Practice Guidelines for Prevention and Management of Avalanche and Nonavalanche Snow Burial Accidents,* Wilderness Medical Society 2024.

10 R. Szynowski (red.), *Ratownictwo górskie. Edukacja transgraniczna ratowników górskich w Polsce i na Słowacji,* Wydawnictwo Naukowe Akademii WSB, Dąbrowa Górnicza 2022, p. 153-168.

11 A. Kottmann et al., *Quality Indicators for Avalanche Victim Management and Rescue*, MDPI 2021

12 A Lunde, C. Tellefsen, *Patient and rescuer safety: recommendations for dispatch and prioritization of rescue resources based on a retrospective study of Norwegian avalanche incidents 1996–2017*, SJTREM 2019.

development are crucial for the effectiveness of rescue operations and for ensuring the safety of both rescuers and victims during avalanche rescue missions.

In this study, a diagnostic survey was selected as the research method. This is a research tool used to diagnose or assess specific problems, needs, or conditions of individuals or groups. The research technique is based on a questionnaire survey, which focuses on identifying problems or detecting certain features that may require further analysis or intervention. The research tool chosen was an online questionnaire created using Google Forms, which allowed easy access to the selected group of respondents and ensured their anonymity.

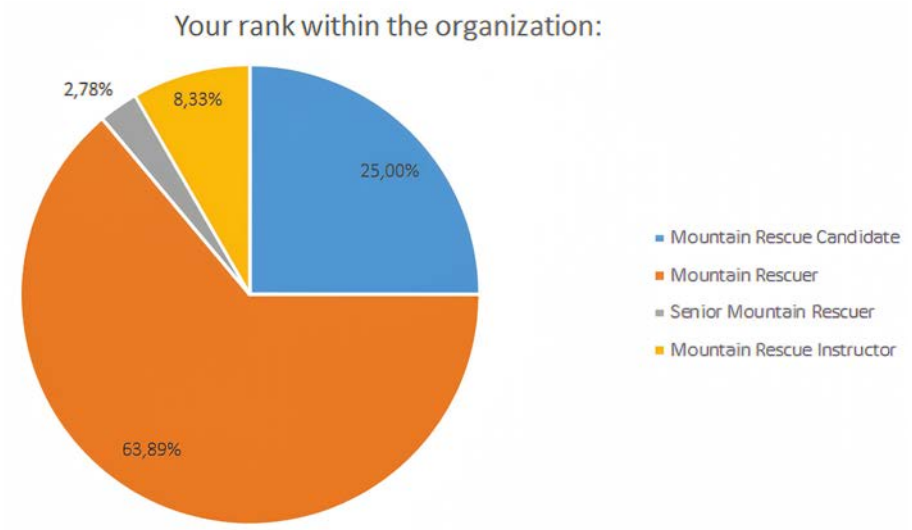
The respondents of this survey were mountain rescuers from the Karkonosze, Podhale, and Bieszczady Groups of the Mountain Volunteer Search and Rescue (polish: Górskie Ochotnicze Pogotowie Ratunkowe – GOPR). These organizations operate in avalanche-prone regions of Poland, and rescuers affiliated with these groups possess the greatest avalanche experience–both theoretical and practical. The questionnaire contained 11 questions aimed at answering the above research question.

Assessment of the Experience and Training of Mountain Rescuers in Avalanche Rescue

The study involved 36 mountain rescuers from all regional GOPR groups. Respondents answered questions in a questionnaire created using the Google Forms tool.

The largest group of respondents (75%) consisted of experienced rescuers: mountain rescuers (63.9%), instructors (8.3%), and senior mountain rescue instructors (2.8%). Candidates for mountain rescuers made up 25% of the participants in the study.

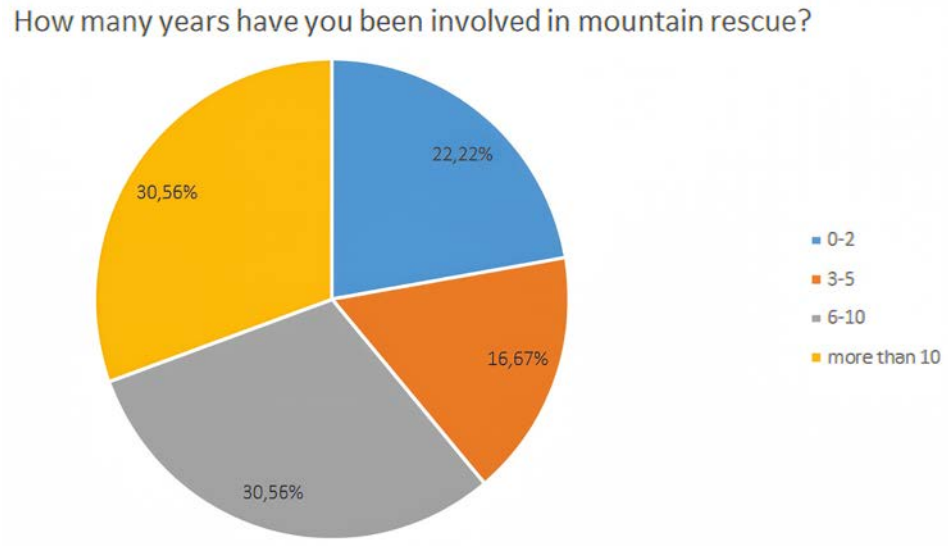
Chart 1. Rank within the organisation



Source: author's own work.

Over 30% of the respondents were rescuers with more than 10 years of experience. The same proportion had more than 5 years of experience. Rescuers with up to 2 years and up to 5 years of experience in mountain rescue accounted for 22.2% and 16.7% of the survey participants, respectively.

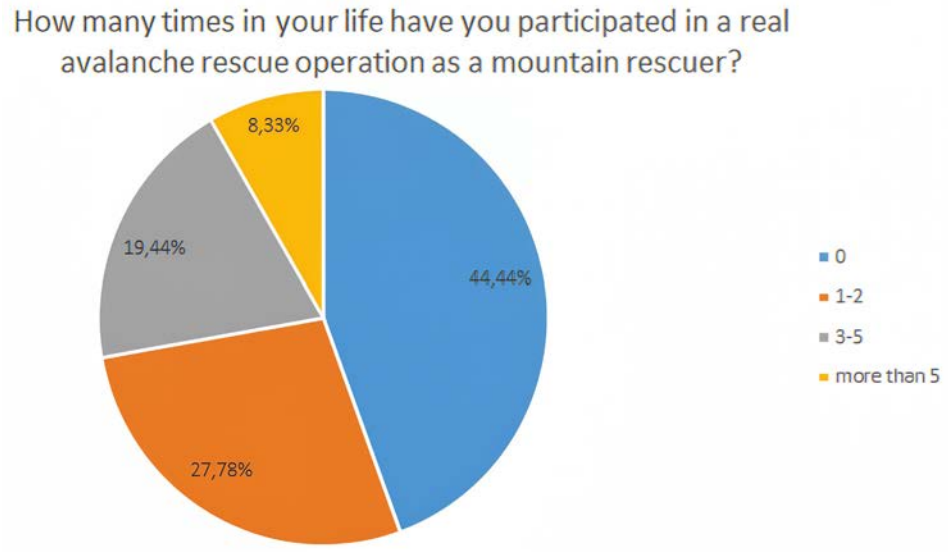
Chart 2. Length of Service in Mountain Rescue



Source: author's own work.

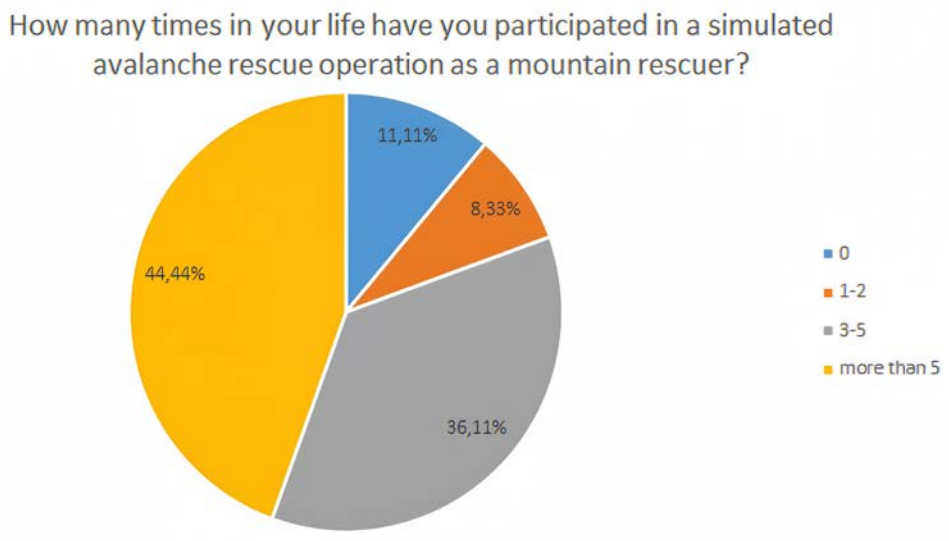
Due to the rarity of avalanche occurrences, nearly 45% of respondents have never had the opportunity to participate in real avalanche rescue operations as mountain rescuers. However, more than half have taken part in such operations at least once. a total of 8.3% of respondents reported participating in more than five real avalanche rescue operations. Nevertheless, the vast majority of rescuers involved in the study have taken part in simulated avalanche rescue scenarios during training exercises.

Chart 3. Participation in Real Avalanche Rescue Operations



Source: author's own work.

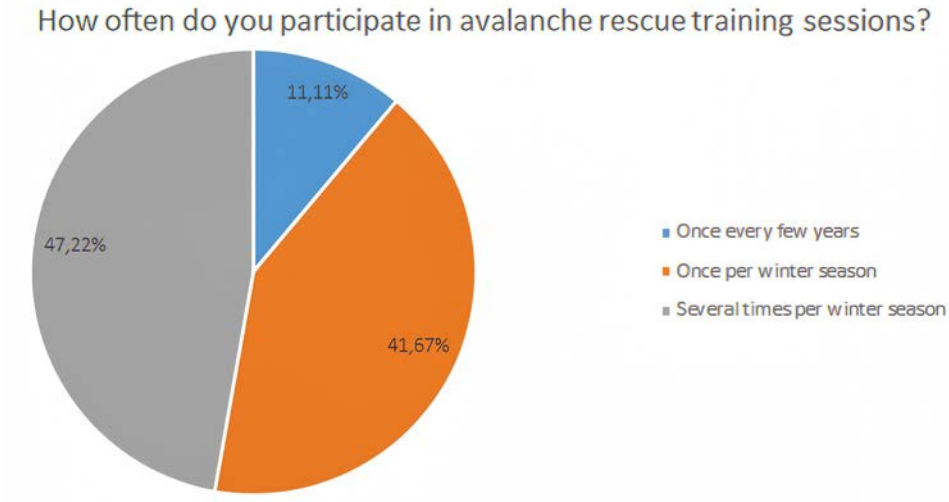
Chart 4. Participation in Simulated Avalanche Rescue Operations



Source: author's own work.

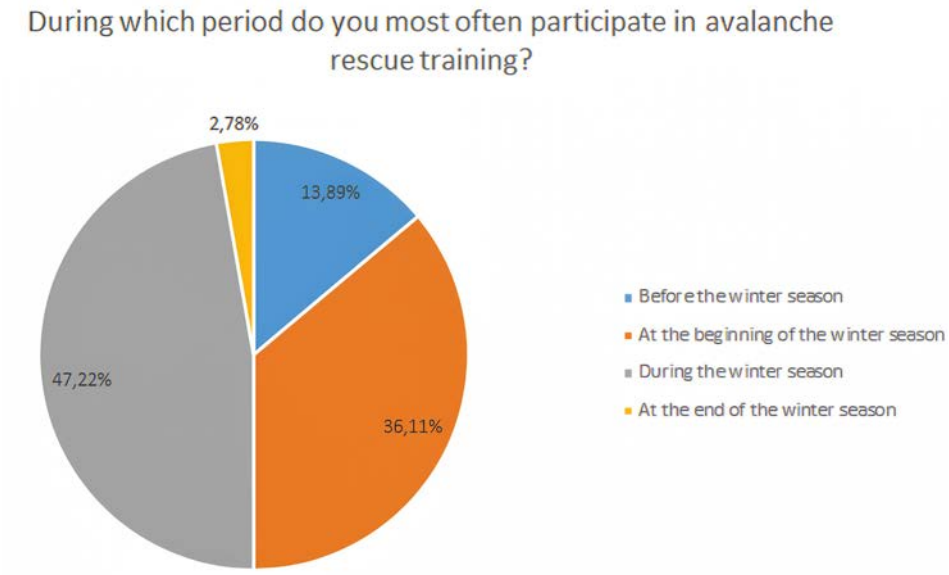
The vast majority of surveyed rescuers (88.9%) declare that they participate in avalanche rescue training at least once per winter season, with more than half of them refreshing this training multiple times throughout the season. Most of the training sessions take place at the beginning and during the winter season.

Chart 5. Frequency of Avalanche Rescue Training



Source: author's own work.

Chart 6. Timing of Avalanche Rescue Training Sessions



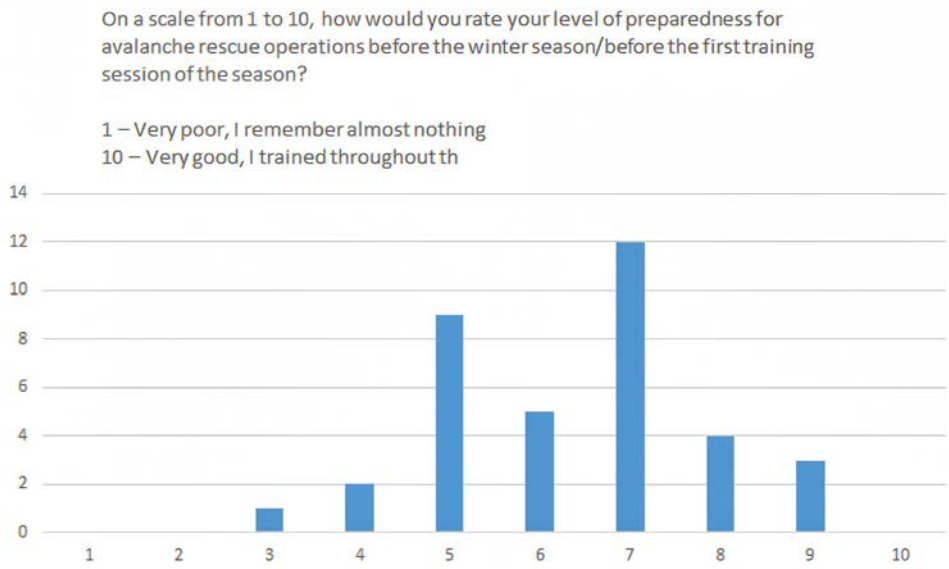
Source: author's own work.

Self-Assessment of Rescuers' Training

Respondents were asked to evaluate their level of preparedness for avalanche rescue operations before the winter season and before the first avalanche training of the season. The assessment was conducted using a 10-point scale, where 1 indicated very poor preparedness and 10 indicated very good preparedness.

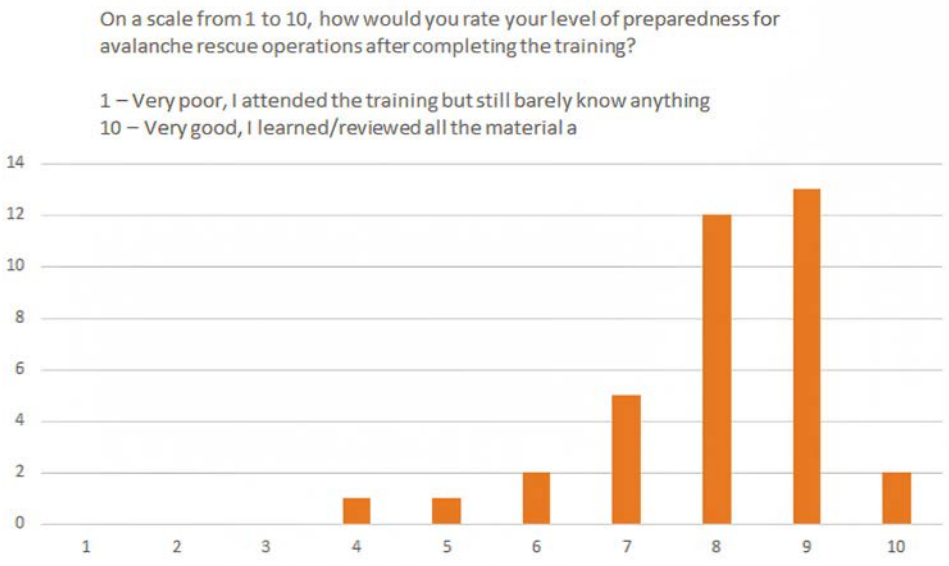
Next, the respondents were asked to assess their level of preparedness for avalanche rescue operations after completing the training, using the same 10-point scale.

Chart 7. Level of Preparedness Before the Winter Season



Source: author's own work.

Chart 8. Level of Preparedness After Training



Source: author's own work.

It is clearly noticeable that attending training before or during the season significantly increases rescuers' level of preparedness for avalanche rescue operations. It is worth noting that a large proportion of rescuers report a decent level of training and readiness (6–9) even before their first training session of the winter season. This reflects their experience and participation in similar trainings over previous years. However, even these experienced rescuers enhance their knowledge, skills, and confidence through regular annual training refreshers.

Rescuers' Opinions on Factors Affecting Safety During Avalanche Rescue Operations

The surveyed rescuers were presented with a series of questions asking them to assess the impact of various factors on safety during avalanche rescue operations. These questions were divided into two groups: factors negatively affecting rescuers' safety and factors positively influencing their safety.:

1. To what extent do the following factors NEGATIVELY affect the safety of rescuers during avalanche rescue operations?
   - strong wind
   - rainfall
   - snowfall
   - intense sunlight
   - night work
   - steep slope gradient
   - difficult access to the incident site
   - working with unfamiliar people
   - working with unknown equipment
   - lack of adequate rescuer training
2. To what extent do the following factors POSITIVELY affect the safety of rescuers during avalanche rescue operations?
   - absence of wind
   - good visibility
   - working during the day
   - working with familiar people
   - working with equipment known to me
   - good rescuer training
   - rescuers equipped with avalanche transceivers
   - well-organized avalanche rescue operation
   - marking the avalanche area with flags
   - keeping a register of people working in the avalanche zone
   - identification of rescuers with numbered armbands

For both questions, a 5-point scale was used to assess the respondents' awareness of factors affecting safety during avalanche rescue operations:

1 – do not affect at all
2 – have some effect, but are not significant
3 – no opinion
4 – have a strong effect
5 – have a very strong and significant effect
The results of the study are presented in the tables below:

Table 1. Assessment of Factors Negatively Affecting Safety

To what extent do the following factors NEGATIVELY affect the safety of rescuers during avalanche rescue operations?					
FACTOR	**1**	**2**	**3**	**4**	**5**
strong wind	0	2	3	15	16
rainfall	0	1	3	18	14
snowfall	1	4	2	11	18
intense sunlight	0	6	8	16	6
night work	0	6	4	13	13
steep slope gradient	0	1	5	9	21
difficult access to the incident site	0	2	4	12	18
working with unfamiliar people	0	10	11	9	6
working with unknown equipment	2	6	8	10	10
lack of adequate rescuer training	1	1	3	10	21

Source: author's own work.

Table 2. Assessment of Factors Positively Affecting Safety

To what extent do the following factors POSITIVELY affect the safety of rescuers during avalanche rescue operations?					
FACTOR	**1**	**2**	**3**	**4**	**5**
absence of wind	0	8	3	10	15
good visibility	0	0	2	19	15
working during the day	0	3	5	15	13
working with familiar people	0	3	5	11	17
working with equipment known to me	0	2	3	14	17
good rescuer training	0	1	0	10	25
rescuers equipped with avalanche transceivers	0	0	3	5	28
well-organized avalanche rescue operation	0	0	1	5	30
marking the avalanche area with flags	1	3	6	12	14
keeping a register of people working in the avalanche zone	0	2	5	12	18
identification of rescuers with numbered armbands	0	4	7	13	12

Source: author's own work.

The third question asked respondents to express their opinion on the following statements:

- Avalanche rescue training only needs to be completed once in a lifetime.
- Avalanche rescue training should be conducted regularly, preferably before or at the beginning of the winter season.
- The quality and type of equipment do not matter during an avalanche rescue operation.
- Using equipment familiar to the rescuer increases the safety of rescuers on the avalanche site.
- Weather conditions during an avalanche rescue operation have a significant impact on safety at the avalanche site.
- Assigning one or more people to continuously observe the slope and avalanche area increases the safety of rescuers working there.

- The use of modern avalanche transceivers by rescuers increases their safety.
- The occurrence of a secondary avalanche affecting rescuers is very unlikely and can be neglected in risk assessment.
- If the operation leader assesses that entering the avalanche site is too dangerous, the rescue operation should be postponed until conditions improve.
- Good planning and management of the avalanche rescue operation by an experienced person increases the safety of rescuers.
- Thoroughly reviewing the avalanche bulletin before the rescue operation increases the safety of rescuers.

For this question, a 5-point Likert scale was used to assess the extent to which rescuers agreed with the given statements:

1 – Strongly disagree
2 – Rather disagree
3 – No opinion
4 – Rather agree
5 – Strongly agree

Table 3. Respondents' opinion on the submitted statements

Please indicate the extent to which you agree with the following statements regarding rescuer safety on the avalanche site:					
STATEMENT	**1**	**2**	**3**	**4**	**5**
Avalanche rescue training only needs to be completed once in a lifetime.	34	1	0	0	1
Avalanche rescue training should be conducted regularly, preferably before or at the beginning of the winter season.	0	0	0	7	29
The quality and type of equipment do not matter during an avalanche rescue operation.	18	3	1	7	7
Using equipment familiar to the rescuer increases the safety of rescuers on the avalanche site.	0	0	2	6	28
Weather conditions during an avalanche rescue operation have a significant impact on safety at the avalanche site.	0	0	1	7	28
Assigning one or more people to continuously observe the slope and avalanche area increases the safety of rescuers working there.	0	1	1	8	26
The use of modern avalanche transceivers by rescuers increases their safety.	0	0	1	6	29
The occurrence of a secondary avalanche affecting rescuers is very unlikely and can be neglected in risk assessment.	28	4	1	1	2
If the operation leader assesses that entering the avalanche site is too dangerous, the rescue operation should be postponed until conditions improve.	2	2	1	15	16
Good planning and management of the avalanche rescue operation by an experienced person increases the safety of rescuers.	0	0	2	5	29
Thoroughly reviewing the avalanche bulletin before the rescue operation increases the safety of rescuers.	0	2	4	6	24

Source: author's own work.

Based on the conducted analysis, it can be concluded that the awareness of mountain rescuers regarding safety during operations carried out in avalanche terrain is at a high level. The survey results clearly indicate that the rescuers are able to accurately identify both factors that promote and threaten the safety of rescue operations under avalanche conditions. The majority of respondents disagree with the statement that attending avalanche training once in a lifetime is sufficient, which demonstrates a widespread understanding of the necessity for regular skills improvement and knowledge updating–especially prior to the winter season.

Respondents place great importance on meteorological conditions and terrain configuration, recognizing them as significant determinants of risk. a clear majority of participants acknowledge the importance of proper planning, management of the rescue operation by experienced leaders, and the use of modern technologies (e.g., avalanche transceivers) as elements that significantly enhance safety. Furthermore, rescuers are aware of the threat posed by secondary avalanches and are willing to suspend operations if the risk is deemed too high–indicating a rational approach to hazard assessment.

The conclusions from the analysis clearly show that key factors for rescuer safety include: high-quality training, familiarity with equipment, effective communication within the team, and continuous monitoring of weather conditions and avalanche bulletins. Such attitudes and beliefs align with current safety standards in high-mountain rescue operations and form the foundation of effective and safe rescue interventions in avalanche terrain.

Conclusions

This study characterized the mechanism of avalanche formation and the factors influencing their initiation. It was emphasized that avalanches are dynamic and multifactorial phenomena, whose occurrence is determined by, among others, the structure of the snow cover, slope angle, meteorological conditions (wind, precipitation, sunlight), and human activity. Special attention was given to the impact of weather and environmental variability as risk factors for both bystanders and the rescuers themselves. In the context of safety, it was demonstrated that secondary avalanches pose a real threat to search and rescue teams, which is also confirmed by the survey responses.

Analyzing the above data allows us to answer the initial research question: How do the experience and training level of mountain rescuers affect their awareness of hazards and their safety during rescue operations in avalanche terrain?

The analysis shows that rescuer safety during avalanche operations results from their knowledge, experience, equipment familiarity, and good team organization.

Based on responses from 36 mountain rescuers, it can be concluded that their training level and awareness are high. As many as 88.9% of participants declare attending avalanche training at least once per season, with over half participating

multiple times. Before the season, rescuers assess their readiness as moderate, but after training, their confidence and competence noticeably increase.

The survey results clearly indicate that rescuers::

- are aware of hazards related to adverse weather and terrain conditions (e.g., strong wind, precipitation, slope steepness),
- appreciate the importance of good organization, equipment knowledge, and working with an experienced team,
- recognize the need for regular training and are willing to suspend operations under extremely dangerous conditions.

The vast majority of respondents reject statements suggesting that a single training or random equipment is sufficient for safe operation. Almost unanimously, they agree that modern avalanche transceivers, proper organization, and knowledge of avalanche bulletins significantly enhance safety.

The hypothesis was formulated that as the level of rescuers' training in avalanche rescue increases, their safety during rescue operations improves. The author also referred to retrospective studies by Lunde and Tellefsen (2019), which emphasized the need to minimize the time rescuers spend in hazard zones to enhance their safety. The analysis was based on survey data collected from GOPR rescuers with significant avalanche operation experience in Poland.

The research hypothesis was confirmed–high training levels significantly reduce risk for rescuers. Additionally, regular training, conscious decision-making, and the use of modern technical equipment form the foundation for safe and effective rescue operations in avalanche conditions.

Bibliography

Andrusikiewicz W., Ratownictwo górskie w kontekście narażenia zawodowego, conference materials, AGH 2023.

Ballesteros-Cánovas J. A. et al., Climate warming enhances snow avalanche risk in the Western Himalayas, PNAS 2018.

Berwyn B., How Climate Change May Influence Deadly Avalanches, SCIAM 2021.

Kacperek M., Kochaj śnieg – unikaj lawin, Kraków 2004.

Kottmann A. et al., Quality Indicators for Avalanche Victim Management and Rescue, MDPI 2021

Kurzeder T., Feist H., Lawinen. Risiko-Check fur Freerider, Insbruck 2012.

Lunde A., Tellefsen C., Patient and rescuer safety: recommendations for dispatch and prioritization of rescue resources based on a retrospective study of Norwegian avalanche incidents 1996–2017, SJTREM 2019.

Nabi H., How climate change worsens avalanches in the Himalayas, Dialogue Earth 2023.

O'Baron A., Clelland M., a Guide To Staying Safe In Avalanche Terrain, 2012.

Szynowski R. (red.), Ratownictwo górskie. Edukacja transgraniczna ratowników górskich w Polsce i na Słowacji, Wydawnictwo Naukowe Akademii WSB, Dąbrowa Górnicza 2022.

Van Tilburg C. et al., Wilderness Medical Society Clinical Practice Guidelines for Prevention and Management of Avalanche and Nonavalanche Snow Burial Accidents, Wilderness Medical Society 2024.

About the Author

Albert Kościński (M.Sc.) – Captain of the State Fire Service, senior rescue specialist, and search dog handler. a certified paramedic and mountain rescuer (GOPR), specializing in search and rescue as well as high-angle rescue operations. Participant in numerous national and international initiatives related to specialized rescue, including rescue missions conducted outside the territory of the Republic of Poland.

Justyna Czopek, MA
WSB University in Dąbrowa Górnicza
e-mail: justyna.czopek2@gmail.com
ORCID: 0009-0006-3033-7554

DOI: 10.26410/SF_2/25/12

CHALLENGES IN THE AREA OF PUBLIC SAFETY FOR THE MAŁOPOLSKA PROVINCE

Abstract

In the face of various threats, such as natural disasters, pandemics, and technical incidents, it is important to have an integrated approach to crisis management that takes into account the specific needs of the region. Therefore, this article focuses on identifying the main challenges and threats of the 21st century that may lead to crisis situations. The analysis covers global trends, such as climate change, as well as local threats specific to the Małopolska Province, including dangers related to infrastructure, ecology, and social aspects. The presentation of specific crisis aspects in Małopolska, identifying the main threats and previous cases of crises, was preceded by a detailed description of the region, taking into account its demography, geography, and infrastructure, which allowed for a better understanding of the unique challenges facing the Małopolska Province. It should be emphasized that the article is an introduction to further scientific considerations focused on the analysis of strategies, structures, and actions taken by the authorities and institutions responsible for crisis management in Małopolska.

Keywords

Threats, public safety, Małopolska Province, Małopolska

Introduction

Crisis is an inherent part of the modern world, affecting both public institutions and local communities. In the face of a growing number of threats, such as climate change, natural disasters, cyberattacks, and pandemics, crisis management is becoming a key aspect of ensuring security and social stability. The Małopolska Province, as one of the most important regions in Poland, is not immune to these challenges. The rich history, dynamic economic development, and diverse geographical landscape of this area require special attention and effective crisis management strategies. In the 21st century, the world has faced constant changes that radically shape social, economic, and political reality. The dynamics of events and global crises are only the tip of the iceberg, representing the challenges that local communities around the world must face.

Characteristics of the region

The Małopolska Province is located in southern Poland and is characterized by diverse topography, which is both an advantage and a potential source of crisis risks. The Małopolska Province consists of 22 counties (including 3 cities with county rights), 182 municipalities, and 1,915 villages. There are 62 cities and 1,951 rural localities within its territory, and the entire province is located at the intersection of important transport routes. The tourist, entertainment, and historical accessibility of the Małopolska region is guaranteed by good transport infrastructure. The area has railways, national roads, and other transport routes running from east to west and from north to south. In the south, the province reaches the state border. It borders the Silesian Province (273.4 km to the west), the Świętokrzyskie Province (178.4 km to the north), the Subcarpathian Province (177.9 km to the east) and the Slovak Republic (301.6 km to the south). The area of the Małopolska Province is 15,182.87 km^2, which accounts for 5% of the area of Poland. The Małopolska Province currently has 3,428,900 inhabitants, 1,640,200 in cities and 1,768,700 in rural areas. Małopolska is home to representatives of ethnic minorities: Karaites, Lemkos, Roma, and Tatars. The population density is 226 people per km^2.

Krakow, a royal city, serves as the capital of this province. Extraordinary landscapes, unique nature, an impressive number of monuments, and a unique atmosphere – all this attracts millions of tourists from Poland and around the world to visit this region every year. As a result, Małopolska has long been one of the most visited regions in Poland. It is worth noting that the Małopolska Province is the leader in terms of the number of licensed mountain guides and hotels. "Małopolska is a region of extraordinary wealth and historical and landscape values, as well as a rich cultural past, perceived as an important center of cultural activity in Poland." Małopolska is an area with a diverse topography. The lowest point is 130 m above sea level, while the highest point, Rysy, reaches 2,499

m above sea level and is the highest peak in Poland. The southern part of the region includes the Tatra and Beskid mountain ranges. The Tatras are the only alpine mountains in Poland, while the Beskids are a gentler range of flysch mountains, rich in forests, fields, and floodplains formed in the valleys. The limestone Pieniny Mountains with the Dunajec River Gorge, a natural monument of global importance, are another important element of the landscape of Małopolska. The central part of the province is crossed by the Vistula, Poland's largest river, which forms a natural border between the mountains and the lowlands in this area. To the north of the Vistula lies the Kraków-Częstochowa Upland, known for its limestone outcrops, gorges, and caves. Among the most famous formations are Hercules' Club in Pieskowa Skała and the Prądnik Valley, located near Ojców. Another unique attraction is the Błędowska Desert, the only desert of its kind in Europe. Małopolska is also known for its complex of Landscape Parks of the Małopolska Province, which includes 11 landscape parks, such as the Beskid Mały Landscape Park, the Bielańsko-Tyniecki Landscape Park, and the Popradzki Landscape Park. These parks protect the unique natural and landscape values of the region. The Małopolska Province attracts numerous tourists thanks to its wealth of monuments and traditions. In May, the Małopolska Cultural Heritage Days are held, during which tourists can visit monuments that are not normally accessible. A special attraction is the Wooden Architecture Trail, which includes 250 buildings, such as churches, Orthodox churches, bell towers, old Polish manors, wooden villas, and open-air museums, where concerts are organized in the summer. The Eagles' Nests Trail with its gorges, ruins of fortresses and castles, the Gothic Trail, the Małopolska Jewish Trail with synagogues, Jewish cemeteries and tenement houses, the Lemko Orthodox Church Trail and the Salt Trail are other routes that attract lovers of history and culture.

The Małopolska region is unique in terms of the number and diversity of monuments that attract tourists from all over the world. Among them are castles, manors, and other places of great historical and cultural value. The Wawel Royal Castle in Krakow is one of the most important places in Polish history. It was the residence of Polish kings and is a symbol of national identity. Its majestic architecture, rich interiors, and Wawel Cathedral, the place of coronation and burial of many Polish monarchs, make it a must-see for every tourist. Visitors can see, among other things, the royal chambers, the armory, and the crown treasury. The castle in Niepołomice, often called "the second Wawel," is another gem of Małopolska. Located in the picturesque surroundings of the Niepołomice Forest, this castle served as a summer royal residence. Today, in addition to visiting the historic interiors, tourists can take part in numerous cultural events, such as concerts and art exhibitions, which take place within its walls. The picturesque castle in Nowy Wiśnicz , built in the Renaissance style, impresses with both its architecture and its picturesque location. It is the second largest castle in Małopolska. Surrounded by a beautiful park, the castle offers visitors the opportunity to travel

back in time thanks to its richly decorated interiors and a museum that presents the history of the region and the Lubomirski family, the former owners of the castle. Jan Matejko's manor house in Koryznówka is a place of special significance for art lovers. It was here that the great Polish painter spent his summer holidays, and today there is a museum dedicated to his life and work. Visitors can admire the artist's original works, as well as numerous family memorabilia that give an insight into Matejko's everyday life. Ignacy Paderewski's manor house in Kąśna Dolna is the only surviving house in the world where this outstanding pianist, composer, and politician lived. The manor house is surrounded by a beautiful park, and its interiors have retained their original furnishings. Numerous concerts and cultural events are held here, referring to Paderewski's rich musical heritage. The Jewish cemetery in Bobowa is an extraordinary place, full of contemplation and reflection. It is one of the most important testimonies to the presence of the Jewish community in Małopolska. With its historic tombstones (matzevot), the cemetery is a valuable historical and cultural monument, reminding us of the rich tradition and history of Polish Jews. Wysowa Zdrój, in addition to its spa qualities, also offers monuments of great religious and cultural significance. Two historic Orthodox churches – St. Michael the Archangel Church and the Church of the Protection of the Holy Virgin – delight visitors with their architecture and unique iconostases. These wooden temples are examples of the region's excellent craftsmanship and sacred art. Each of these places not only enriches the historical and cultural knowledge of visitors, but also offers unforgettable experiences and insight into the rich heritage of Małopolska. From monumental castles to intimate manor houses and memorial sites, this region is a real treasure trove for all those who wish to explore its history and traditions.

The Małopolska Province, rich in monuments, beautiful landscapes, and tourist attractions, attracts millions of tourists from Poland and abroad every year. The most important cities in Małopolska are Wadowice, the hometown of Pope John Paul II, Miechów with the wooden manor house of Tadeusz Kościuszko and the Basilica of the Holy Sepulchre, Tarnów with its medieval old town, Nowy Sącz with one of the largest market squares in Poland, and Kraków, rich in historical monuments. Oświęcim, known throughout the world for the former Nazi death camp Auschwitz, today serves as an important place of remembrance and education about the Holocaust. Its natural and cultural wealth, as well as its developed tourist infrastructure, make Małopolska one of the most visited regions in Poland, both by tourists and students attracted by its renowned universities. The area also offers unique experiences for all mountain lovers. The region, which is part of the historical area of Małopolska, has lowland and mountainous areas, including the Tatra Mountains, Pieniny Mountains (Tropical Mountains), and Beskids. Despite potential hazards, the mountainous region of the Małopolska Province is very often the most popular tourist destination and natural attraction, attracting thousands of tourists from all over the world.

Crisis aspects in the Małopolska Province

In the southern part of this region, there is a possibility of many crisis threats due to its mountainous terrain. Extreme weather events, such as heavy rains or rapid warming, can cause floods, landslides, avalanches, construction, transport, industrial, and environmental disasters. The level of security in the Małopolska Province is also influenced by external factors related to Poland's participation in military and stabilization operations in a "hot" region, the war in Ukraine, the unprecedented increase in the threat of terrorism in Europe and worldwide, and the recent COVID-19 pandemic.

Mountainous areas are particularly vulnerable to such phenomena due to steep slopes and changes in topography, which can lead, for example, to local crises hindering communication, access to cities, and care for the injured. Let us also consider the risks associated with mountain tourism. Especially during periods of increased tourist traffic in summer and winter, mountain regions become crowded, which can contribute to infrastructure overload and pollution, as well as an increase in the number of accidents and missing tourists. In the event of bad weather or a mountain accident, rescue operations can be hampered by difficult terrain, requiring greater coordination of rescue services and adequate preparation for such situations. Proper planning, monitoring, and risk management are therefore essential to minimize the impact of potential geological hazards while ensuring the safety and protection of the region's unique natural heritage, and are also necessary for natural disaster management and to ensure an integrated approach to crises.

The province is picturesque and interesting, but it is also exposed to various natural disasters that can lead to regional crises and emergency situations requiring a quick and effective response. Floods are one of the greatest threats to the Małopolska Province, especially during periods of heavy rainfall or sudden snowmelt. This is one of the most common natural hazards, constituting an extreme, often violent and unusual natural phenomenon. According to Article 16(43) of the Act of July 20, 2017 - Water Law, a flood is defined as "the temporary covering of an area that is not normally covered by water, in particular caused by the swelling of water in natural watercourses, water reservoirs, canals, and from the sea, excluding the covering of an area caused by the swelling of water in sewage systems." In low-lying areas, especially along the Vistula River and its tributaries, flooding can occur, causing significant material and human losses. In the past, this region has experienced numerous floods that have damaged homes, roads, bridges, and infrastructure, as well as caused crop and human losses. The mountainous areas of the Małopolska Province, which include the Tatra, Pieniny, and Beskid Mountains, are prone to landslides and avalanches, especially during periods of heavy snowfall and rapid temperature changes. These phenomena can block roads, destroy infrastructure, and even endanger human life. The flood risk level is 15% higher than the average flood risk in Poland and covers about 50% of the province's area. The total length of rivers and streams

is about 6,000 km. Natural lakes are found only in the Tatra Mountains. In addition, high mountains are susceptible to sudden atmospheric changes, which can lead to sudden weather changes and storms, increasing the risk of avalanches and landslides. Another threat that the Małopolska Province may face, especially in summer, is heat waves and drought, and extreme temperatures can cause heat waves, threatening the health and lives of people, especially the elderly and the sick.

Droughts in the region have become increasingly frequent in recent years and can lead to crop damage, loss of water resources, and deterioration of living conditions for residents. Finally, storms, gales, and hailstorms are further phenomena independent of human factors that can pose a threat to the Małopolska Province and its inhabitants. Severe storms are often accompanied by gusty winds and heavy rainfall, which can damage buildings, knock down trees, break power lines, and cause transportation disruptions. Hailstorms accompanied by thunderstorms can destroy crops, cars, buildings, and injure people outdoors. To effectively prepare for extreme weather events, Poland, and especially the Małopolska Province, must implement emergency plans, invest in warning systems (such as the RCB), and monitor and train local communities so that they know how to deal with the threats they face. Appropriate precautions and emergency response can help minimize the effects of potential disasters.

However, high tourist traffic, especially seasonal traffic, can be both an opportunity for development and a potential threat to the region. First, infrastructure overload is a major challenge for the Małopolska Province. During the peak tourist season, tourist infrastructure such as roads, parking lots, and hiking trails can become congested, especially in the vicinity of Krakow and the Tatra Mountains. The influx of tourists can lead to traffic jams, difficulties in accessing tourist attractions, and a deterioration in the quality of life for residents. In addition, increased travel can lead to congestion in public transport and public transport. Environmental pollution is another problem associated with intensive tourism. Increased tourism is often accompanied by increased waste, air pollution, and destruction of natural ecosystems. Especially in mountainous areas where tourism is highly developed, the problem of environmental pollution can be particularly acute, leading to the degradation of nature and threats to local flora and fauna. In addition, excessive exploitation of tourist attractions can lead to soil erosion and loss of biodiversity. When it comes to tourist traffic in the Małopolska Province, the safety of tourists is also a serious threat, as the terrain is often difficult and unpredictable, and tourists are exposed to various hazards such as injuries, accidents, and disappearances. Sudden changes in weather, failure of tourist equipment, or inadequate preparation can lead to critical situations requiring the intervention of emergency services. In addition, an increase in the number of tourists may result in an increase in criminal incidents, such as theft and property damage, which may affect the sense of security of tourists and residents. Another challenge associated with tourism is social conflict. Intensive tourism can lead to social conflicts between residents and tourists, especially in cases of public

disorder, environmental pollution, or safety violations. These conflicts can affect the social atmosphere, negatively influence the perception of tourists, and increase tensions between different social groups. Therefore, tourism management and related tourism infrastructure planning are of great importance in minimizing the effects of potential tourism-related crises. Preventive measures, tourism education, and coordinated actions by emergency services and local governments can contribute to ensuring tourist safety and sustainable development in the Małopolska Province.

The Małopolska Province is characterized by a diverse landscape, ranging from lowlands to mountainous areas, and is rich in unique ecosystems that are an important part of the local natural and cultural heritage. However, the protection of the natural environment in the Małopolska Province faces many threats that can lead to ecosystem degradation, loss of biodiversity, and negative effects on human health. The first threat to environmental protection in the Małopolska Province is environmental pollution. Population growth and intensive industrial and transport development can lead to the release of harmful substances into the atmosphere, surface waters, and soil. This pollution negatively affects the quality of air, water, and soil, which in turn negatively affects human health, quality of life, and ecosystem functioning. Another threat is the degradation of natural ecosystems, especially those in rural and mountainous areas, and the increased consumption of natural resources, particularly water and energy. Overuse of natural resources, deforestation, urbanization, and the expansion of tourist infrastructure can lead to the loss of nature.

The Małopolska Province is characterized by a diverse landscape, ranging from lowlands to mountainous areas, and is rich in unique ecosystems that constitute an important element of the local natural and cultural heritage. However, environmental protection in the Małopolska Province faces many threats that can lead to ecosystem degradation, loss of biodiversity, and negative effects on human health. The first threat to environmental protection in the Małopolska Province is environmental pollution. Population growth and intensive industrial and transport development can lead to the release of harmful substances into the atmosphere, surface waters, and soil. This pollution negatively affects the quality of air, water, and soil, which in turn negatively affects human health, quality of life, and ecosystem functioning. Another threat is the degradation of natural ecosystems, especially those in rural and mountainous areas, and the increased consumption of natural resources, particularly water and energy. Overuse of natural resources, deforestation, urbanization, and the expansion of tourist infrastructure can lead to the loss of natural habitats for many plant and animal species and a reduction in biodiversity. The degradation of ecosystems can lead to the destabilization of local ecosystems, reduced resilience to climate change, and the loss of ecosystem services essential to human well-being. The Małopolska Province, like other regions, often faces problems related to drinking water shortages, water pollution, and excessive energy consumption. Uncontrolled industrial, agricultural, and tourism development can lead to excessive consumption of resources, which in turn can lead to their depletion and negative effects on the

environment and human health, while climate change poses a serious challenge to environmental protection throughout the province. Rising temperatures, changes in precipitation, extreme weather events, and rising sea levels can have serious environmental, economic, and social consequences. The increase in the frequency and intensity of extreme weather events such as floods, droughts, and storms can lead to an increased risk of natural disasters and loss of natural resources. Therefore, protecting the natural environment of the Małopolska Province requires coordinated action at the local, regional, and national levels. Preventive measures, investments in sustainable development, public education, and effective environmental protection regulations can help minimize the impact of potential threats to natural and human health. Appropriate adaptation to climate change and the promotion of pro-environmental attitudes are key to maintaining ecological balance and sustainable development in the Małopolska Province.

Summary

In the face of various threats, such as natural disasters, pandemics, or technical incidents, it is important to have an integrated approach to crisis management that takes into account the specific needs of the region. Therefore, this article focuses on identifying the main challenges that pose potential threats to the local community, using the example of the Małopolska Province. It should be emphasized that this article is an introduction to further scientific considerations focused on the analysis of strategies, structures, and actions taken by local authorities and institutions responsible for crisis management in Małopolska.

Bibliografia

Awarie i katastrofy budowlane spowodowane warunkami atmosferycznymi – czy można ich uniknąć?, https://naszbiznes24.pl/awarie-i-katastrofy-budowlane-spowodowane-warunkami-atmosferycznymi-czy-mozna-ich-uniknac/.

Centrum Paderewskiego https://centrumpaderewskiego.pl/dwor-paderewskiego-1.htm.

Cerkiew świętego Michała Archanioła Wysowa-Zdrój https://narowery.visitmalopolska.pl/web/turystyka-religijna/obiekt/-/poi/cerkiew-sw-michala-archaniola- wysowa-zdroj.

Cmentarze Żydowskie http://cmentarze-zydowskie.pl/bobowa.htm.

Komunikat odnośnie wystąpienia warunków suszy w Polsce https://www.mir.krakow.pl/artykuly/Komunikat-odnośnie-wystąpienia-warunków-suszy-w- Polsce,14782.html.

Kozak M. W., *Typologia konfliktów występujących w sektorze turystycznym*, Warszawa 2016.

Małopolskie Dni Dziedzictwa Kulturowego https://www.malopolska.pl/dla-mieszkanca/kultura-i-dziedzictwo/projekty-i-inicjatywy-kulturalne/malopolskie-dni-dziedzictwa-kulturowego.

Muzeum pamiątek po Janie Matejce – "Koryznówka" – Stary Wiśnicz https://nowywisnicz.pl/muzeum- pamiatek-po-janie-matejce-koryznowka-stary-wisnicz.html.

O Małopolsce https://www.malopolska.pl/dla-mieszkanca/o-malopolsce.

Plan zarządzania kryzysowego województwa małopolskiego, Urząd Wojewódzki, Wydział Bezpieczeństwa i Zarządzania Kryzysowego, Kraków 2024.

Ustawa z dnia 20 lipca 2017 roku, - *Prawo wodne*, Art. 16 pkt. 43 (Dz.U. 2017 poz. 1566).

Wawel https://wawel.krakow.pl/o-wawelu.

Wójtowicz-Wróbel A., *Ochrona* Środowiska *w Małych Miastach Obszaru Metropolitalnego Krakowa – Programy Działań,* Kraków 2007.

Wróbel R., *Zarządzanie ryzykiem na potrzeby systemu zarządzania kryzysowego w Polsce w optyce wymagań Mechanizmu Ochrony Ludności*, Warszawa 2019.

Zadania inwestycyjne w latach 2018-2023 https://www.malopolska.pl/dla-mieszkanca/kultura-i-dziedzictwo/inwestycje-w-kulturze/zadania-inwestycyjne-w-latach-20182020.

Zamek Królewski https://zamekkrolewski.com.pl/zamek-krolewski/historia/.

Zamek Wiśnicz https://zamekwisnicz.pl/.

About the Author

Deputy Director in the Department of Security and Crisis Management at the Małopolska Provincial Office. PhD student at the WSB Academy. Graduate of the Jagiellonian University in Krakow, master's degree in national security. Research interests include national security, crisis management, and the functioning of public administration in the area of civil protection.

Associate prof. Dipankar Haldar, PhD
Serampore College University in India
e-mail: dipankarsmp@gmail.com
ORCID: 0000-0002-3970-8095

Justyna Gach
WSB University in Dąbrowa Górnicza
e-mail: gach.justyna1701@gmail.com
ORCID: 0009-0001-2651-0

DOI: 10.26410/SF_2/25/13

THE APPLICATION OF BIOMETRIC METHODS IN PERSONAL IDENTIFICATION

Abstract

Biometrics, a technique for identifying individuals based on their unique physical and behavioral characteristics, is finding growing use in a variety of fields, notably security systems. This article examines a variety of biometric approaches used in identification procedures, including fingerprint analysis, facial recognition, iris scanning, retina scanning, and voice and handwriting recognition. The operating principles and practical uses of these technologies, such as access control systems, border security, public monitoring, and law enforcement, are discussed. The study evaluates the performance of distinct biometric approaches, as well as their advantages and limits in identity verification. It also covers the difficulties in maintaining biometric databases and how they affect the accuracy and reliability of identification operations. Biometrics, owing to its precision and speed, is recognized as a vital instrument in crime prevention and national security. The study concludes by reflecting on the future of biometrics, the advancement of identifying technologies, and the issues that may arise when biometrics are increasingly implemented in international security systems and identity management.

Keywords

Biometrics, identification, security systems, dactyloscopy, national

Introduction

Identifying and safeguarding human identity has become crucial in the age of digital transformation, the increasing significance of information security, and the pervasive use of mobile and internet-based technologies. In this regard, biometrics – an interdisciplinary discipline that incorporates aspects of computer science, biology, mathematics, statistics, law, and ethics – is one of the fastest-growing sciences. The field of biometrics focuses on identifying and validating people using their distinct biological traits (such as fingerprints, iris patterns, or vascular structures) or behavioral traits (such as voice patterns, typing rhythm, or stride). Unlike traditional passwords, biometric techniques don't need the user to memorize them, which makes them very accurate and resistant to falsification. International standards provide a clear definition of biometrics. The International Organization for Standardization (ISO) defines biometrics as the "Automated recognition of individuals based on their physiological and/or behavioral characteristics"[1]. This implies it is based on who a person is or how they act, rather than what they own (e.g., an access card) or know (e.g., a password). Biometrics is now used in a variety of applications, including national security and military systems, e-banking, border control, healthcare, and ordinary consumer electronics like cellphones, laptops, and payment terminals. Its presence has become almost imperceptible while remaining important. Although biometrics as a scientific area just emerged in the nineteenth century, its origins go far deeper. Biometric features have been used for identification since ancient China, when merchants and authorities signed with their fingerprints. with medieval Persia, physical descriptions of prisoners were documented to aid with identification. In the late nineteenth century, British scientist Francis Galton, a cousin of Charles Darwin, showed the uniqueness of fingerprints and developed the first classification system for them, marking a watershed moment in the development of biometrics as a scientific approach. Around the same period, Alphonse Bertillon created an anthropometric system based on body measurements that was used by police agencies for many years[2]. The subsequent introduction of digital computers and algorithmic methodologies permitted the development of the first automated biometric systems, and the turn of the twentieth and twenty-first century witnessed a surge in the everyday usage of biometric technology[3].

Biometrics now plays an important part in the digital infrastructure of the information society, in addition to serving as an identifying system. However, as it grows in popularity, so does the number of legal, ethical, and societal problems. Biometric data is regarded highly sensitive since it is immutable and directly linked to an

1 A. K. Jain, A. Ross, K. Nandakumar, *Introduction to Biometrics*, Springer, 2011, p. 119.

2 National Research Council. *Biometric Recognition: Challenges and Opportunities*, p. 212.

3 J. Wayman, A. K. Jain, D. Maltoni, and D. Maio, *Biometric Systems: Technology, Design and Performance Evaluation*, p. 198.

individual's identity; once hacked, it cannot be altered or canceled, unlike a password. Furthermore, some biometric technologies, such as face recognition in public places, pose severe concerns regarding surveillance limits, privacy rights, and civil liberties. According to Alessandro Acquisti, a top researcher in privacy and data ethics, "Biometrics are the most reliable identifiers that cannot be lost, forgotten, or changed. That's what makes it so strong and deadly"[4].

In response to these concerns, some governments and international organizations have enacted legislation to protect individual rights. The General Data Protection Regulation (GDPR), also known as the European Parliament and Council Regulation, is the most significant legal legislation controlling the processing of biometric data in Europe. According to GDPR, biometric data used to uniquely identify a natural person is classified as a special category of personal data that is generally prohibited from being processed unless specific legal grounds exist, such as explicit consent, public interest, employment necessity, or national security. GDPR also requires data controllers to follow principles such as data minimization (processing only what is necessary), implementing appropriate technical and organizational safeguards, and allowing individuals to exercise their rights, which include access to, correction, deletion, and objection to the processing of their data[5].

Biometrics, while technically sophisticated and full of potential, is not a neutral phenomenon; its advancement necessitates a constant balancing act between identification system efficiency and the safeguarding of basic human rights. The current user of biometric technology frequently unknowingly leaves traces of their identity not just online but also in databases whose security is critical to avoiding abuse. As a result, any introduction to biometrics must go beyond the technological and practical elements, taking into account the social, ethical, philosophical, and legal settings. Only then can we completely comprehend the importance of biometrics and its role in defining the future of human-technology interactions[6].

The current development of biometrics is bringing us closer to a scenario in which the distinction between physical and digital identity is becoming increasingly blurred. Access to services is increasingly granted using the distinctive aspects of our own bodies – our face, voice, eyes, or hands – rather than papers, passwords, or codes. In light of this shift, a fundamental issue arises: are we, as a society, ready for such a profound integration of our physical selves with technology? The solution is far from straightforward. On the one hand, biometrics provides great convenience, increases security, and lowers the chance of fraud. On the other hand, it requires complete faith in the organizations that collect and handle our data, as well as assurance that the methods used to identify us would not be used against us in the future.

4 S. Rane, Y. Wang, S. C. Draper and P. Ishwar, *Secure Biometrics: Concepts, Authentication Architectures and Challenges*, p. 326–339.

5 M. Faundez-Zanuy, J. Fierrez, M. A. Ferrer, M. Diaz, R. Tolosana and R. Plamondon, *Handwriting Biometrics: Applications and Future Trends in e-Security and e-Health*, p. 87.

6 Ibid., p. 108.

Biometrics' future will be influenced not just by technology improvement, but also – and maybe more importantly – by public discussion, law, organizational ethics, and civic consciousness[7].

As a result, one of the most pressing tasks in the coming years will be not only the continued refinement of biometric algorithms, but also the development of what could be referred to as "technological ethics," as well as user education about their rights and the potential threats posed by the misuse of biometric data. Engineers and developers are not the only ones responsible for the future of this sector; legal experts, educators, sociologists, and philosophers are all involved and, most importantly, users must learn to evaluate the technology they use critically. In a world where "our body becomes our password," as many technological pundits now claim, we require a new level of awareness and alertness. Biometrics is more than just a technology; it is also a reflection of our societal values, attitudes toward privacy, and the extent to which we respect human dignity in the digital era[8].

In a larger sense, biometrics has become a symbol of the evolving interaction between humans and technology. Algorithms are increasingly processing our bodies, emotions, and movements, converting them into data that is then used to validate our identities. Rather of being recognized for our tales, words, or experiences, we are more identifiable by our appearance or behavior. This transition poses fundamental problems, such as whether technology allows us to express ourselves or reduces us to patterns and statistics. Are we still people creating our own identities, or are we becoming objects of incessant analysis? As biometric systems gain strength and popularity, we must determine whether we want a future based on trust and freedom or control and monitoring. That is why it is critical to create biometric technology in a way that preserves fundamental values such as privacy, dignity, and individual autonomy[9].

We must also remember that biometrics does not emerge in a vacuum; rather, it evolves within a social and political environment. Engineers, governments, companies, and individuals all have influence on how it is utilized. History has proven that even the most promising technology may be exploited if protections are not in place. This is why we need clear standards, more public knowledge, and open conversations about how biometric data is gathered and used. Biometrics is more than simply a technology; it holds significant power and responsibility. We must question ourselves whether we want a world in which biometrics make us safer and more empowered, or one in which they limit our freedom. In the end, how we utilize biometric technology will be a test–not only for science and law, but for society as a whole–to see if we can maintain our humanity in a more digital environment[10].

7 Ibid., p. 209

8 R. R. Sokal and F. J. Rohlf, *Introduction to Biostatistics*, 2nd ed., p. 78.

9 J. Wayman, A. K. Jain, D. Maltoni and D. Maio, *Biometric Systems: Technology, Design and Performance Evaluation*, p. 48.

10 Ibid., p. 76

Types of methods

Biometric technologies are among the most advanced and successful methods for identifying and authenticating persons in both digital and physical systems. Unlike traditional security measures such as passwords or PIN codes, biometrics are based on the examination of individual qualities that are unique to each individual and exceedingly difficult to duplicate or fabricate. Biometric systems may use both physical and behavioral features, increasing their adaptability and extending their range of applications. In practice, a number of biometric approaches are used, each adapted to the unique demands of the company, desired security level, and ambient conditions.

These approaches are often divided into two categories: static techniques, which study permanent physical aspects, and dynamic techniques, which focus on human activities. Static biometric approaches provide greater accuracy and long-term consistency, whereas dynamic methods provide continuous identification verification throughout user activities. Regardless of the technology employed, the process entails collecting biometric data, processing it, extracting differentiating characteristics, and comparing the results to a stored reference template. Advanced artificial intelligence and machine learning algorithms offer more precise matching and lower false acceptance or rejection rates[11].

Biometric systems are utilized in both the public and private sectors, ranging from access control and transaction authorization to surveillance and national security identification. These technologies are increasingly often combined with mobile and cloud-based systems, making them acceptable for everyday applications while yet providing high levels of data security. However, deploying biometric technology raises legal and ethical concerns, notably around user privacy and accountability for any breaches. The system's ability to withstand spoofing assaults and other cybersecurity risks is a key consideration.

Biometrics' high efficacy originates from the difficulty of copying an individual's unique traits, which serve as a type of "access key." Well-designed systems may significantly lower the danger of illegal access while improving overall information and asset security. Different biometric approaches offer varied degrees of accuracy, reliability, and user ease, which is why hybrid systems that combine numerous techniques are frequently used. These combinations improve the system's resilience and flexibility to changing environmental circumstances[12].

In recent years, dramatic breakthroughs in digital technology and device downsizing have allowed biometrics to be applied on an unprecedented scale. Modern systems provide real-time user authentication, which is becoming increasingly crucial in light of rising cybersecurity risks and the need to secure sensitive data. It's also worth noting that the success of a biometric system is determined not only by the

11 R. R. Sokal and F. J. Rohlf, *Introduction to Biostatistics*, 2nd ed., p. 211.
12 Ibid., p. 139.

underlying technology, but also by the quality of the input data, the environment in which it is gathered, and the security with which the biometric templates are maintained. Biometrics have enormous promise for automating security procedures and maintaining identities, but successful deployment necessitates appropriate infrastructure, user education, and compliance with data protection requirements.

These technologies provide a high level of security and accuracy by analyzing unique physical or behavioral characteristics that are difficult to forge, with ideal examples including the face, iris, fingerprint, hand geometry, voice, signature, and scent, while biometric methods use these features to reliably identify or authenticate individuals, finding wide application in security systems across both the private and public sectors.

Facial Recognition Technology: Principles, Applications, and Ethical Implications

The biometric approach of facial recognition includes studying the unique anatomical characteristics of the human face in order to identify or authenticate an individual. These systems process a face picture using cameras and powerful algorithms before comparing it to a database-stored template. These methods examine key traits such as eye distance, nose shape, jawline contour, and face proportions. Facial recognition may work in both static and dynamic situations (for example, passport images and real-time surveillance). The fact that this technology is contactless and user-friendly is one of its most significant advantages. This technology is utilized in cellphones, airports, access control systems, and city monitoring. Despite its great accuracy, facial recognition may face obstacles due to illumination, facial emotions, or partial face occlusion. Concerns have also been raised concerning privacy and the possibility for select organizations to misuse this technology. As a result, it is critical to appropriately control its usage and safeguard the security of users' biometric information. Facial recognition technology is continually advancing, and contemporary systems can recognize and analyze faces in crowds, from a distance, and from different perspectives. Artificial intelligence and machine learning are increasingly being utilized to increase accuracy and minimize identifying mistakes. In certain nations, similar technologies are also employed to fight crime and track down wanted persons. Facial recognition is used in the private sector to personalize services, such as in retail and marketing. This strategy is projected to become even more popular in the future, but there will also be an increase in demand for solutions that assure transparency and ethical use of technology[13].

Iris Pattern Recognition: Precision-Based Identification in High-Security Environments

Iris recognition is a very accurate and secure biometric identification technology. The iris, the colorful region of the eye that surrounds the pupil, has a distinct pattern that remains consistent throughout a person's lifetime. Even identical twins have varied

13 M. A. Turk, A. P. Pentland, *Eigenfaces for Recognition*, *Journal of Cognitive Neuroscience*, 1991, p. 71–86, available online: https://watermark.silverchair.com/jocn.1991.3.1.71.pdf [accessed: February 18, 2025].

iris patterns; therefore, this procedure is quite dependable. The method works by taking a high-resolution image of the eye with specialized cameras, frequently employing infrared light to emphasize the iris' complex intricacies. The collected pattern is then transformed to mathematical code and compared to data stored in a database. This approach has an extremely low mistake rate, both in terms of rejections and false acceptances. It is therefore often utilized in high-security settings including airports, military installations, and government buildings. Furthermore, iris scanning is quick, contactless, and user-friendly. The iris does not deteriorate or wear out with frequent use like fingerprints do. Additionally, the system is very resistant to efforts at deception, including the use of pictures or artificial eye replicas. However, the expense of implementation and the requirement for accurate imaging equipment are two of the difficulties. However, iris recognition is becoming more widely available because to technological developments, and it is being utilized more often in commercial applications such as payment systems and cellphones. All things considered, iris recognition is regarded as one of the most reliable biometric techniques now in use[14].

Fingerprint Analysis in Biometric Systems: Accessibility, Accuracy, and Challenges

One of the most popular and practical biometric identification techniques is fingerprint-based. Since each person has a distinct fingerprint pattern, this technology is extremely accurate and difficult to counterfeit. In order to authorize access, the fingerprint is scanned and compared to a previously saved template. Depending on the equipment, several technologies, such as optical or ultrasonic sensors, can be used for the scan. We frequently employ this technique to get entry to guarded facilities, unlock phones, and enter into bank accounts. It is quick and doesn't require password memory, which is convenient for a lot of people. It's not flawless, though; occasionally if a finger is damp, unclean, or damaged, the scanner won't be able to read the fingerprint. Security issues also arise since, unlike passwords, you cannot simply "reset" your fingerprint data if it is stolen. To increase security, this technique is frequently used in conjunction with other biometric technologies, such as facial recognition. Artificial intelligence is currently used by more sophisticated systems to improve accuracy and function better under various circumstances. However, the more biometric data we get, the more crucial it is to adequately preserve it, both legally and technically[15].

Hand Geometry-Based Identification: Mid-Security Biometric Solutions in Practice

The method which is related to biometric and use the geometry of a hand is the use of the biometrics of hand geometry. In Hand-geometry, the attributes are based on the shape, length and width of the finger and the ratio of different parts in the hand,

14 M. Goc, J. Moszczyński, *Polish Society of Criminology*, Warsaw, 2007, p. 36.

15 R. Sanchez-Reillo, C. Sanchez-Avila, A. Gonzalez-Marcos, *Biometric Identification Through Hand Geometry Measurements*, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pp. 1188–1191, available online: https://ieeexplore.ieee.org/document/879796 [accessed: February 18, 2025].

as opposed to fingerprint patterns on papillary lines. This invention can tolerate minor skin injury, or dirt. Hand geometry-based systems are fast, user-friendly, and, in general, non-invasive. Handprint recognition system can be used in medium secure areas, access control of building or time attendance system also to the gym. During the enrollment, the user's hand is scanned once and saved in a system in the form of a pattern. For verification, the user presses his or her hand onto a dedicated scanner and the current image is compared to a reference image that had been previously stored. One of the benefits of the approach is that it suffers very low failure rate and it is also less costly to implement on the ground. Even when operating with a large number of users, these systems perform well. While it is true that hand geometry is not as singular as an iris or fingerprint, it is secure enough for most applications. The technology conveniently excels where speed and user comfort are concerned. This method's somewhat lesser accuracy when compared to more sophisticated biometric approaches is a disadvantage. Furthermore, hand geometry-based systems necessitate direct physical contact with the scanner, which in some circumstances may be deemed unsanitary. Hand geometry recognition is still a common and useful option for many businesses in spite of this[16].

Voice Biometric Authentication: Voiceprints, Vulnerabilities, and Technological Progress

Voice biometric identification is an authentication technique that uses an analysis of an individual's distinctive speech patterns. Pitch, tone, speed, accent, and timbre are some of the unique characteristics of the human voice that make it challenging to mimic. These characteristics are used by speech recognition software to generate a distinct voiceprint that is linked to a certain person. Voice registration and real-time voice comparison are usually the two steps in the procedure. Voice recognition makes contactless and easy authentication possible, in contrast to more conventional techniques like passwords or PIN numbers. Numerous applications use it, such as access control, customer service systems, cellphones, and telephone banking. Crucially, these systems may function in both passive and active modes, requiring the user to pronounce a certain word. Notwithstanding its benefits, this technology has drawbacks. Background noise, throat conditions, voice fatigue, and the speaker's emotional state can all have an impact on recognition accuracy. Anti-spoofing features are frequently included in contemporary systems due to worries about possible fraud involving voice recordings or artificial voices. However, thanks to developments in machine learning and artificial intelligence, speech biometrics is always getting better. It is a desirable identification approach, particularly in situations like distant identity verification where other biometric techniques are less useful[17].

16 A. Służewska, *Methods of Visualizing Fingerprint Traces on the Metal Surface of Cartridge Cases – a Brief Review*, *Problemy Kryminalistyki*, 2007, No. 257, Warsaw, 2007, p. 47.

17 M. Kulicki, V. Kwiatkowska-Wójcikiewicz, L. Stępka, *Forensic Science. Selected Issues of Criminal and Judicial Investigative Theory and Practice*, Toruń, 2009, p. 324–330.

Dynamic Signature Recognition: Behavioral Biometrics in Legal and Financial Contexts

Analyzing each person's signature's distinct features is the foundation of the biometric signature recognition technique. Biometric systems examine dynamic characteristics including pen pressure, writing speed, rhythm, and angle, in contrast to conventional handwritten signatures that are readily falsified. Biometric signatures are far more secure since these criteria are hard to copy. This approach makes use of specialized tools, such as digital pens or graphic tablets, that record intricate information while the sign is being made. Banks, government agencies, insurance providers, and other sectors requiring safe and trustworthy identification verification utilize signature recognition. Since many individuals are used to signing documents, this method's naturalness and social acceptance are among its main advantages; it doesn't feel invasive. Furthermore, it is simple to include a biometric signature into already-existing electronic documents. Nevertheless, this approach may be susceptible to changes in writing style brought on by stress, sickness, or exhaustion. As a result, biometric systems need to be calibrated correctly and have a margin of tolerance. Biometric signatures are becoming more and more popular as an addition to or substitute for conventional authentication techniques in spite of these drawbacks. These systems have two modes of operation: identification mode, which compares a signature to several templates in a database, and verification mode, which compares a signature to a stored template. Therefore, biometric signatures may be used to legally sign electronic documents and to verify identification. The increasing need for automated and secure identification systems is satisfied by this technology[18].

Olfactory Biometrics: Experimental Approaches to Human Scent-Based Identification

Based on each person's own fragrance, olfactory biometrics holds promise as an identifying technique. Each smell is distinct and is released by the human body as a result of sweat gland activity, skin bacteria, and other variables. Specialized tools, including chemical sensors, are needed to use this technology. These tools analyze and identify fragrance molecules in order to provide a biometric profile. This approach has drawbacks even though fragrance is hard to fake. The accuracy of identification can be impacted by a person's changing fragrance due to dietary changes, stress, medicine, and other environmental circumstances. Nevertheless, olfactory biometrics finds use in domains including environmental research, medical diagnostics, and security. As technology develops, it may become more popular and support other biometric techniques like fingerprint or face recognition. For this reason, despite the challenges associated with its use, olfactory biometrics could become an innovative tool in improving security and the accuracy of identification processes across various industries.

18 J. Gach, A. Tavares, *Fingerprinting as a Biometric Identification Tool: Methods and Applications in Modern Forensic Science*, *Security Forum*, 2024, No. 2.

Technical, Legal and Societal Challenges of Biometric Identification Systems

Biometrics is becoming a regular part of our daily lives – from unlocking phones, online banking, to airport security systems. It seems fast, convenient, safe, and modern. And to be fair, it does have a lot of advantages. But, as with most technology, things aren't always as perfect as they seem. Biometric sciences come with a number of serious downsides, many of which are overlooked or ignored. Before we fully embrace them, it's worth taking a closer look at the risks involved. Setting up a biometric system is expensive. You need hardware to scan faces, fingerprints, or irises, along with proper software and security infrastructure.

These technologies don't come cheap, which limits access for many institutions. It feels like this type of security is only for those who can afford it, creating a gap in availability and fairness. Biometrics doesn't work everywhere or in every condition. If it's dark, dirty, or if the equipment glitches – facial or fingerprint recognition might fail. In criminal investigations, it's even trickier[19]. Gathering high-quality biometric evidence at a crime scene isn't always possible. Rain, poor lighting, dust – and suddenly the entire system is useless. Skin damage, scars, illness, or just the natural aging process can make it hard for the system to recognize someone. And what about people without fingers, hands, or with facial deformities? For them, biometric tech simply doesn't apply. Sometimes, humans just don't fit the system. Additionally, biometrics isn't always as quick as claimed. Analysis in police or financial systems may take a while. The technology moves at its own speed and doesn't always live up to our expectations. The longer it takes to receive a result, the more complicated the case. Data leaks are one of the main issues. You can change your password if it is stolen. However, if someone manages to obtain your fingerprints or face information, you will be permanently affected. You cannot change your hands or face. Unfortunately, hackers may still affect even the most protected systems. Then there is the possibility of misidentification[20]. Not every technology is flawless. It's possible for a system to mistakenly identify someone, accusing an innocent person or allowing the wrong person to escape punishment. Errors like this can have major repercussions in high-stakes situations like courtrooms or airports. Another major warning sign is surveillance. Presumably for safety, facial recognition cameras are becoming more and more common in public areas, but sometimes without the knowledge or approval of the public. You may never be aware that you are being followed. That poses a serious risk to individual privacy. Speaking of permission, you frequently have no actual say in the matter. Do you want to utilize this service or app? Enter your biometric information. Do you not want to? You

19 R. R. Sokal and F. J. Rohlf, *Introduction to Biostatistics*, 2nd ed, p.138.
20 Ibid., p 176.

can't access it then. What a waste of voluntary involvement. Furthermore, biometric technologies have the potential to discriminate. They don't give everyone the same recognition[21]. Elderly people, children, and those with darker skin are frequently mistaken. In the end, a purportedly impartial technology serves to strengthen already-existing societal injustices. Profiling can also be done with biometric data. Businesses may create thorough behavioral profiles by examining a person's gait, speech, and gadget usage. They can then sell this information to insurance companies or advertisements. It invades your personal life and goes beyond identification. The absence of control is another problem. You have no idea where your biometric information is kept, who may access it, or what happens to it once it is publicly available. The way these mechanisms' function lacks sufficient accountability and transparency. The psychological aspect cannot be disregarded either. Your behavior changes when you are aware that you are being watched all the time. You begin acting differently because the system "expects" it to, not because you want to. It produces a steady, silent pressure. Not to be overlooked are the technological malfunctions. Biometrics can malfunction or crash like any other technology. When it happens, you may lose access to your personal phone, bank accounts, and buildings. Convenience soon becomes a major issue. The public's lack of trust is also getting worse. Without knowing how biometric systems operate or how their data is secured, people feel compelled to use them. More openness and education are desperately needed; else, mistrust and fear will only increase[22].

The Future of Biometrics: Innovation, Regulation, and Digital Identity Transformation

In reality, no one can truly predict what the future of biometrics will look like; we can only speculate on possible outcomes. However, looking at the history of this field, the future appears to be both promising and crucial, especially as people become increasingly connected to the internet and digital systems with each passing day. Governments are also becoming more technology-friendly, with some administrative offices now accessible only through fingerprint or iris recognition. Initially, biometrics was associated solely with fingerprints or facial geometry, but as the science has evolved, identification is now also possible through scent or handwriting. Each of these methods is becoming increasingly advanced and complex.

Currently, researchers focus their work primarily on identification through voice tone, behavioral analysis, facial emotion recognition, and even the patterns of veins in the hands or on the body, as well as the way a person moves. These

21 R. R. Sokal and F. J. Rohlf, *Biometry: The Principles and Practice of Statistics in Biological Research*, 1973, p. 228.
22 Ibid., p. 312.

complex, multi-layered biometric systems not only allow for effective authentication but also enable the prediction of user behavior, which can be applied in areas such as cybersecurity, medicine, elderly care, and marketing. In biometric science, a key advantage is that the same principles can be applied across fields like forensics, psychology, and even healthcare. That is why I personally believe biometrics should be a more widely taught and understood area of knowledge. Unfortunately, with every mention of evolution or development, the word challenge inevitably follows. When it comes to biometrics, this challenge is closely tied to privacy protection and data security. The lesson here goes beyond passwords, PINs, or logins – it involves personal identifiers that, once exposed, can be exploited by criminals, with no option to delete or reset them. This means that security measures must be significantly more sophisticated, and the legal regulations governing the storage, processing, and sharing of data must become both standardized and stricter. This will require cooperation between technology developers, governments, and organizations focused on personal data protection, who must find a balance between innovation and responsibility[23]. Decentralized systems are already emerging–based on blockchain or zero-knowledge proof architectures – that allow identity verification without revealing full biometric data. These approaches could become the new standard in the future. Biometrics are somewhat like a swing – they can both increase and decrease the sense of security. On one hand, in authoritarian states such as North Korea, China, or Iran, biometrics are used to excessively monitor citizens, creating fear among people that they are under constant government surveillance, almost like machines. On the other hand, in democratic countries, biometrics help combat cybercrime. Therefore, building public trust through education, clear legislation, and choice will be essential–users should have real control over what data is collected and for what purpose[24]. In the long term, biometrics may cease to be merely a method of authentication and instead become an integral part of our digital identity–enabling not only access to services but also fostering personalized interactions with technology that increasingly understands our needs, emotions, and habits.

Summary

Biometrics has become an increasingly common part of modern life, offering fast, efficient, and personalized ways to verify identity through unique physical and behavioral traits. Whether it's unlocking a phone, accessing a bank account, or passing through airport security, biometric systems are designed to make life easier and more secure. However, this convenience comes with significant

23 J. Gach, A. Tavares, *Fingerprinting as a Biometric Identification Tool: Methods and Applications in Modern Forensic Science*, *Security Forum*, 2024, No. 2.

24 D. Krishna, F. A. Talukdar, and R. Laskar, *Study on Biometric Authentication Systems, Challenges and Future Trends: a Review*, p. 12.

challenges. The key concern is that biometric data is permanent – unlike passwords, you can't change your fingerprints or face. If such data is stolen or misused, the consequences can be long-lasting. Issues like lack of user consent, poor data transparency, and potential misuse by governments or corporations make it clear that biometrics is not just a technical tool, but also a social and ethical issue. Surveillance and discrimination are also major risks. Not all biometric systems treat users equally, and some can reinforce social biases. Public spaces monitored by facial recognition may improve security, but they also raise serious privacy concerns. Without strong legal protections and public understanding, we risk creating systems that control rather than protect. For this reason, the future of biometrics must be built not only on technological progress but also on responsibility, fairness, and transparency.

Governments must enforce strict data regulations, companies must prioritize user privacy, and individuals must be aware of their rights. Biometrics has the potential to support a safer and smarter world – but only if we ensure it works for people, not against them. Its true success will depend on how well we balance innovation with human dignity and democratic values.

Bibliography

Faundez-Zanuy, M., Fierrez, J., Ferrer, M. A., Diaz, M., Tolosana, R., & Plamondon, R. (n.d.). Handwriting biometrics: Applications and future trends in e-security and e-health.

Gach, J., & Tavares, A. (2024). Fingerprinting as a biometric identification tool: Methods and applications in modern forensic science. Security Forum, (2).

Goc, M., & Moszczyński, J. (2007). Polish Society of Criminology. Warsaw.

Jain, A. K., Ross, A., & Nandakumar, K. (n.d.). Introduction to biometrics.

Kolano, W., & Tavares, A. (2022). The role of Poland in ensuring European security. Security Forum, 6(1), 21–34.

Krishna, D., Talukdar, F. A., & Laskar, R. (n.d.). Study on biometric authentication systems, challenges and future trends: a review.

Kulicki, M., Kwiatkowska-Wójcikiewicz, V., & Stępka, L. (2009). Forensic science: Selected issues of criminal and judicial investigative theory and practice. Toruń.

National Research Council. (n.d.). Biometric recognition: Challenges and opportunities.

Rane, S., Wang, Y., Draper, S. C., & Ishwar, P. (n.d.). Secure biometrics: Concepts, authentication architectures and challenges.

Sanchez-Reillo, R., Sanchez-Avila, C., & Gonzalez-Marcos, A. (n.d.). Biometric identification through hand geometry measurements. IEEE Transactions on Pattern Analysis and Machine Intelligence. Available online: https://ieeexplore.ieee.org/document/879796 [Accessed: February 18, 2025].

Służewska, A. (2007). Methods of visualizing fingerprint traces on the metal surface of cartridge cases – a brief review. *Problemy Kryminalistyki*, (257). Warsaw.

Sokal, R. R., & Rohlf, F. J. (1973). Biometry: The principles and practice of statistics in biological research.

Sokal, R. R., & Rohlf, F. J. (n.d.). Introduction to biostatistics (2nd ed.).

Turk, M. A., & Pentland, A. P. (1991). Eigenfaces for recognition. Journal of Cognitive Neuroscience, 3(1), 71–86. Available online: https://watermark.silverchair.com/jocn.1991.3.1.71.pdf [Accessed: February 18, 2025].

Wayman, J., Jain, A. K., Maltoni, D., & Maio, D. (n.d.). Biometric systems: Technology, design and performance evaluation.

About the Authors

Dipankar Haldar, PhD, Associate Professor of Serampore College University, India.

Justyna Gach, Vice-Chair of the Main Board of the International Scientific Association for Security "Save the World". Her academic interests focus on issues related to security systems, criminal forensics, and the role of technology in contemporary identification processes.

Dominika Grzybowska-Ganszczyk, PHd
Jerzy Kukuczka Academy
of Physical Education in Katowice
e-mail: dominikagrzybowska@yahoo.com
ORCID: 0000-0002-6413-306X

Bartosz Głowacki, PHd
Jerzy Kukuczka Academy
of Physical Education in Katowice
e-mail: b.glowacki@awf.katowice.pl
ORCID: 0000-0001-6453-2039

Jakub Ganszczyk, MsC
Laboratorium Badań Balistycznych
i Urządzeń Wyposażenia Strzelnic
e-mail: kubaganszczyk@yahoo.com
ORCID: 0009-0001-0541-1963

DOI: 10.26410/SF_2/25/14

SAFETY AT THE SHOOTING RANGE DURING FIREARMS TRAINING PROTECTION OF THE LOCAL POPULATION AND RISK MINIMIZATION

Abstract

The article presents a comprehensive overview of safety principles applicable during firearms training. It discusses key organizational, technical, and psychophysical factors influencing participant safety, including equipment, clothing, mental and physical condition, experience level, and the instructor's role. The text emphasizes adherence to weapon control procedures, communication protocols in emergencies, and the establishment of safe zones. Special attention is given to medical preparedness, including first-aid equipment, communication with duty officers, and knowledge of emergency procedures. The study also highlights the importance of systematic training evaluation, debriefing, and experience sharing among instructors.

The conclusion indicates that a high level of safety in firearms training can only be achieved through consistent application of safety rules, proper course organization, and continuous improvement of both participant and instructor competencies.

Keywords

safety, firearms training, instructor, procedures, medical support, psychophysical readiness, training organization

Introduction

Safety constitutes one of the most crucial aspects in the organization of training sessions, courses, and workshops related to the handling of firearms. This issue concerns both civilians developing their skills in the field of sport shooting and individuals who perceive firearms as tools of personal protection. Although firearms are gradually ceasing to be a social taboo and are becoming increasingly accessible, their use continues to require a responsible attitude and a high level of user awareness[1]. The growing interest in firearms training stems not only from easier access to information but also from the rising public awareness of the importance of safe weapon handling skills[2].

The motivations of individuals applying for firearm permits are highly diverse. For some, shooting represents a hobby; for others, a form of recreation or a continuation of family traditions associated with hunting. For a considerable group of individuals, firearms serve as instruments of sporting competition or as a means of enhancing personal safety competencies[3]. a relatively small percentage of applicants cite threats to life or health as the primary reason for obtaining a firearms license.

A specific group within this context consists of minors participating in sport shooting competitions. Their training must take into account not only age-related restrictions concerning the type of firearm and shooting discipline but also the need for particular attention to safety-related aspects[4]. In such cases, the priority lies not merely in the acquisition of shooting techniques, but primarily in the formation of proper habits and attitudes concerning the responsible use of firearms and ammunition.

1 A. Idzikowski, *Szkolenie strzeleckie. Bezpieczeństwo – charakterystyka zagadnienia*, Legionowo 2014.

2 K. Konopka, *Prawo i bezpieczeństwo na strzelnicach publicznych*, „Magazyn Policji KSP" 2022.

3 *Ogólne zasady bezpieczeństwa obowiązujące przy uprawianiu sportu strzeleckiego*, Polski Związek Strzelectwa Sportowego (PZSS).

4 *Bezpieczeństwo na strzelnicy – podstawowe zasady*, Warszawa 2025.

Safety rules during training

Every individual applying for a firearm license must undergo mandatory theoretical and practical training, completed with a state examination as well as medical and psychological assessments. The training encompasses the knowledge of legal regulations, principles of safe firearm handling, and practical shooting skills. This requirement applies to all user groups – civilians, sport shooters, hunters, security personnel, firearm collectors, and law enforcement officers alike.

However, obtaining a firearm license should not be regarded as the culmination of the training process. Each firearm owner is obliged to continuously improve their skills, both technical and related to the safe operation of weapons. This requirement is not only of a legal nature but also of an ethical one – as a firearm owner bears responsibility for their own safety and that of their surroundings.

The instructor's role and responsibilities

The instructor, trainer, or teacher conducting the classes plays a pivotal role in the teaching process. The duty to properly prepare and conduct training in a manner that ensures maximal participant safety falls squarely on them. This responsibility encompasses both methodological and organizational preparation – selecting the venue and timing of the training, determining the number of participants, providing necessary equipment, and assessing the skill level, knowledge, and psychophysical condition of trainees. The training content should always be adapted to the participants' level of advancement. a different approach is required for athletes who train regularly under a coach's supervision than for recreational groups or beginners who are frequently encountering a firearm for the first time. In the case of such groups, particularly at commercial shooting ranges, the instructor should exercise increased vigilance and caution when admitting participants to live firing[5].

A separate category comprises the training of uniformed-service personnel, whose curricula and training procedures are regulated in detail by statutory instruments and internal departmental regulations[6]. Despite a high level of oversight and professional preparation of staff, incidents may still occur in such environments as a result of routine or momentary lapses in concentration. For this reason, one should always apply the principle of limited trust, maintain a high level of vigilance, and respond decisively to any deviations from established safety rules[7]. Hazardous situations may arise not only during shooting activities themselves but also during routine handling of firearms – for example, during cleaning, maintenance, or adjustment of sighting devices. The most frequent cause of accidents is routine and the belief in "complete control" over the weapon. Therefore, every user, regardless

5 A. Kaczmarski, *Organizacja systemu szkoleń strzeleckich w polskiej Policji*, „Securitologia" 2017.

6 *Ustawa z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej* (Dz.U. z 2013r. poz. 628).

7 *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 26 sierpnia 2014 r. w sprawie szczegółowych zasad szkolenia strzeleckiego funkcjonariuszy Policji* (Dz.U. z 2014 r. poz. 1195).

of experience, should continuously rehearse basic safety rules, intervene when observing unsafe behaviour in others, and refine their habits regarding the responsible handling of firearms.

Preparation of the instructor. General principles of preparation

The instructor should prepare methodologically, organizationally, and technically, with due attention to safety aspects. Key tasks include:

1. inspection of the technical condition and safety of firearms and ammunition;
2. preparation of firing points and the shooting area in accordance with safety principles (designation of safe zones, movement routes, muzzle-direction corridors);
3. preparation of medical and alarm safeguards (first-aid kit, designated first-contact personnel, evacuation plan, contact with the facility's medical staff);
4. risk analysis related to individual characteristics of participants (experience, psychophysical condition, possible medical contraindications).

In the case of mixed groups with varying levels of proficiency, the instructor should:

- introduce an individualized lesson program and initial familiarization exercises;
- divide participants into subgroups according to skill level and training objectives;
- provide additional instructional staff or assistants for beginner groups.

Procedures for unloading firearms and depositing ammunition before activities

Prior to the commencement of activities, particularly tactical training conducted outside a specialized shooting range, the instructor must order the mandatory deposit of ammunition (and, if necessary, personal firearms) in a secure location (safe, armoured cabinet) under the supervision of a designated person.

Practical guidelines:

- Instructor's commands when collecting ammunition: "Unload the weapon and magazines," "Deposit ammunition – to the safe." Magazines must be unloaded. Fig. 1.

Fig. 1. Unloading a magazine.

Source: own elaboration

- Place loose ammunition in a bag/container or in an ammunition "basket" and deposit it in the safe. Figs. 2, 3, 4.

Fig. 2. Placing ammunition in an ammunition "basket."

Source: own elaboration

Fig. 3. Placing loose ammunition in a bag.

Source: own elaboration.

Fig. 4. Depositing ammunition in the safe.

Source: own elaboration.

- "Unloading" ammunition is understood as the removal of all rounds from each magazine; it does not merely mean detaching the magazine from the firearm.

Three-stage weapon check – procedure and commands

To ensure maximal safety, a three-stage weapon-check system is proposed.

Stage I – Self-check by the participant ("self-check")

Procedure

1. The instructor issues the command: "Inspect your weapon." The participant inspects the magazines (to verify they contain no rounds and are not damaged), Fig. 5. Empty magazines are placed in the designated area.

Fig. 5. Magazine prepared for inspection.

Source: own elaboration.

2. The participant draws the firearm from the holster, points the muzzle toward a safe direction, and keeps the index finger aligned along the slide (safe finger position). Fig.6.

Fig. 6. Safe finger position on the firearm.

Source: own elaboration.

3. The participant disengages the safety (if an external safety is fitted), retracts the slide to its rearward position, visually verifies that the chamber is empty (holding the slide open for 2–3 s), and then releases the slide. Fig. 7.

Fig. 7. Disengaging the safety.

Source: own elaboration.

4. The participant fires a control shot toward a designated safe backstop (an instructor command is required if the object for the control shot has been designated). Fig. 8.

Fig. 8. Performing a control shot.

Source: own elaboration.

5. The participant secures the firearm and returns it to the holster.

Notes: throughout the entire procedure the muzzle must remain pointed in a safe direction; the instructor supervises and corrects any irregularities.

Stage II – Instructor check ("unload for inspection")

Procedure

1. The instructor issues the command: "Unload for inspection."
2. Designated persons (or all participants simultaneously) check the magazine and the firearm, lock the slide to the rear (using the slide-stop lever). Fig. 9.

Fig. 9. Slide locked to the rear during firearm inspection.

Source: own elaboration.

3. They raise the firearm so the instructor standing behind them can visually inspect the chamber and magazines. Fig. 10.

Fig. 10. Positioning the firearm for magazine inspection.

Source: own elaboration.

4. The instructor inspects the firearm and magazines. After inspection, the instructor informs each inspected participant: "I have inspected the weapon" and signals the completion by touching the participant's shoulder (procedure used for groups arranged in a line).
5. The participant releases the slide-stop lever, fires a control shot toward a safe backstop, secures the firearm, returns it to the holster, and places magazines in pouches.

Stage III – Mutual inspection by fellow trainees

Procedure (Variant A – on-the-spot inspection):

1. The instructor issues the command: "Show your weapon for inspection to the person on your right/left" or "Unload and show the weapon for inspection."
2. Fellow trainees position themselves so they can safely inspect the adjacent participant's firearm (observing muzzle direction and finger-on-slide rules).
3. After inspection: release the slide, perform a control shot, secure and holster the firearm.

Procedure (Variant B – transfer for inspection):

1. The instructor issues the command: "Prepare the weapon for transfer for inspection," followed by "Pass the weapon for inspection." Participants pass the firearm holding it by the slide/frame (grip area free), while observing the highest safety precautions. Fig.11.

Fig. 11. Handing over a firearm for inspection.

Source: own elaboration.

2. After the weapon inspection, the instructor may issue the command "About-turn – inspect the handed-over weapon." All participants then inspect their fellow trainee's firearm and, upon the subsequent commands "About-turn – return the inspected weapon," they return the inspected firearm while simultaneously reclaiming their own.

Remarks: the handing over of personal firearms to others for inspection should only be practiced with training or dummy weapons. When exercises are conducted using personal firearms, it is preferable to conduct mutual inspection under the owner's supervision without physically transferring the weapon. The fellow trainee inspects the firearm in the same manner as previously performed by the instructor.

Specific instructor commands – standardized phrases

To maintain clarity and training discipline, it is advisable to use a consistent set of standardized commands:

- "Inspect your weapon" – instruction for the participant to conduct a self-check.
- "Unload for inspection" – instruction to prepare the firearm for instructor inspection (slide locked in the rearward position).
- "Show your weapon for inspection" / "Show your weapon for inspection to the person on your [right/left]" – instruction for mutual inspection of firearms.
- "Prepare to hand over your weapon for inspection" / "Hand over your weapon for inspection" – commands related to the transfer of firearms for inspection.
- "Weapon inspected" – instructor's confirmation that the inspection has been completed.

Each command should be delivered clearly, concisely, and in a manner that leaves no ambiguity regarding the expected action.

Inspection of instructor weapons

Instructors are also subject to inspection. The first and second stages of the inspection procedure apply equally to the instructors' firearms, and they should perform these checks simultaneously with the trainees. One or two participants should be designated to carry out the inspection of the instructor's weapon. This procedure reinforces the principle of mutual responsibility and accountability.

Preventive and Protective Measures

1. Equipment and clothing – appropriate attire, protective eyewear, and hearing protection; absence of loose elements that could interfere with firearm handling.
2. Psychophysical condition of participants – the instructor must inquire about and monitor readiness (asking about fatigue, medication, or alcohol consumption).
3. Inspection of additional equipment – checking places where participants might conceal ammunition or tools (pockets, bags).
4. Principle of limited trust – regardless of participants' experience, the instructor should maintain cautious supervision and monitor every deviation from established procedures.
5. Safe unloading zones – especially important during training outside the shooting range; such zones must be designated and clearly marked for unloading and firearm inspection.
6. Ammunition/firearm deposit – firearms and ammunition should be stored in a locked safe or secure cabinet during training, under the supervision of a designated person.

Elements enhancing participant safety

The safety of participants in firearms training depends not only on adherence to technical and organizational principles but also on numerous individual factors such as psychophysical condition, clothing, equipment, and experience level. Neglecting these elements may result in improper training progression, loss of concentration, and consequently – accidents or potentially hazardous situations.

Equipment and clothing

Appropriate clothing and equipment constitute a fundamental component of safety during firearms training. Attire should be suited to the nature of the exercises – comfortable, non-restrictive, and free from loose elements that could catch on the firearm or other equipment. For firearms-related activities, clothing that covers the body, footwear with a stable sole, protective eyewear, and hearing protection are mandatory.

Personal equipment (holster, magazine pouches, tactical belt, vest) should be arranged ergonomically and safely. Improper placement of equipment components may hinder access to the weapon or result in accidental contact with trigger mechanisms.

Before each session, the instructor should inspect participants' attire and equipment, paying attention to:

- • correct attachment of holsters and magazine pouches,
- • stability of tactical belts and vests,
- • proper placement of spare ammunition,
- • absence of decorative or hazardous elements (chains, keyrings, cords).

The instructor's role also includes advising on equipment and clothing selection – a practice particularly common in sport shooting, where the coach assists the athlete in adjusting gear to individual needs[8].

Psychophysical condition of participants

The psychophysical condition of participants is crucial for ensuring safety. Fatigue, stress, lack of sleep, or decreased concentration significantly increase the risk of errors that may lead to firearm-related accidents[9]. Overworked individuals respond more slowly, exhibit reduced hand-eye coordination, and may misinterpret instructor commands.

Before beginning training, the instructor should observe participants, paying particular attention to:

- signs of fatigue, distraction, or emotional agitation,
- delayed responses to commands,
- difficulty maintaining proper posture or rhythm of work.

In case of signs of reduced psychophysical performance, the instructor should:

8 *Ogólne zasady bezpieczeństwa obowiązujące przy uprawianiu sportu strzeleckiego*, Polski Związek Strzelectwa Sportowego.

9 *Bezpieczeństwo na strzelnicy – podstawowe zasady*, Warszawa 2025.

- exclude the participant from active shooting,
- assign them to auxiliary tasks (e.g. "target handler", "role player"),
- suggest rest or consultation with the training supervisor.

Participants should also be aware of their own limitations and report any indisposition to the instructor before starting the exercises.[10]

Level of experience and group diversity

A varied level of participant experience is one of the greatest challenges for an instructor. In groups where there is a wide range of skill levels, the pace and scope of exercises should be adjusted to the capabilities of the least advanced participants, without compromising safety.

It is recommended that:

- before training begins, the instructor conducts a short assessment of participants' skill levels (e.g. a brief dry-fire exercise),
- in large groups, additional instructors supervise specific firing lanes or training zones,
- the instructor positions themselves closest to the least experienced person or team,
- where possible, the level of difficulty of exercises is varied (basic and advanced variants).

Participants with lower skill levels require greater supervision regarding firearm handling, conduct on the range, and reaction to commands. An experienced instructor should continuously monitor the participants' pace, correct mistakes, and prevent any unauthorized changes in positioning or task execution.[11]

Integration of safety factors

Safe training requires that all discussed elements – equipment, clothing, psychophysical condition, and experience – function as a connected system. Even the best-prepared exercise can become dangerous if a participant is fatigued, has an improperly secured holster, or misunderstands commands.

The instructor's responsibilities therefore include:

- maintaining discipline,
- enforcing compliance with safety rules,
- eliminating risk factors,
- conducting exercises at a pace that ensures control over the group.

A high level of safety results from synergy between the instructor's technical preparation, participants' awareness, and proper organization of activities.[12]

10 Szerzej: A. Kaczmarski, *Organizacja systemu szkoleń strzeleckich*…

11 Szerzej: Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 26 sierpnia 2014 r. *w sprawie szczegółowych zasad*…

12 *Wybrane aspekty bezpieczeństwa podczas zajęć z użyciem broni palnej*, Szczytno 2022.

Training security – general principles

Ensuring the safety of firearms training requires strict adherence to safety rules to minimize the risk of accidents and hazards. The key elements include organization of the training area, control of hazardous materials, supervision of participants, and emergency response procedures.

Designating safe zones

The instructor issues the command: "Designate safe zones – no unauthorized persons may enter." Safe zones include: areas for observers, instructor zones, storage areas for equipment, and evacuation corridors. Defining such zones minimizes accidental access to the line of fire and protects bystanders.[13]

Control of access to ammunition and firearms

The instructor issues the command: "Check access to ammunition and firearms – no unauthorized person may have access."

Ammunition and firearms must be stored in locked, marked storage facilities. Issuing them to participants takes place only under supervision of an authorized person. Access control reduces the risk of accidents and theft.[14, 15]

Appointing persons responsible for safety

The instructor issues the command: "Assign safety officers – each zone must have a supervisor." Each training area must have a designated safety coordinator responsible for compliance with procedures and for responding in case of danger. This person monitors participants and can stop the exercise at any time if safety is compromised.[16]

Compliance with communication and emergency procedures

The instructor issues the command: "Communication and alert procedures apply to everyone – report any threat immediately." Training should include clear communication rules: alarm signals, procedures for notifying emergency services, and immediate reporting to the instructor. Observing these procedures enables quick response and limits the effects of incidents.[16]

Effective training security requires precise organization, control of hazardous materials, supervision, and adherence to emergency protocols. Each element of security directly impacts participant safety and the overall effectiveness of training.

---

13 A.Jha & Izaguirre, Mary & Adler, Amy, *Mindfulness Training in Military Settings: Emerging Evidence and Best-Practice Guidance*, Current Psychiatry Reports ,2025, pp 393-407.

14 D. Hemenway & Rausher, Steven & Violano, Pina & Raybould, Toby & Barber, Catherine. *Firearms training: What is actually taught?*, „Injury Prevention" 2027, no 25.

15 R. Renner, Cvetković, V. M., & Lieftenegger, N., *Dealing with High-Risk Police Activities and Enhancing Safety and Resilience: Qualitative Insights into Austrian Police Operations from a Risk and Group Dynamic Perspective* „Safety" 2025, 11(3), 68.

16 J.R. Blalock, Black, R.A., Bourke, M.L. et al., *Emergency Communication Operators: Findings from the National Wellness Survey for Public Safety Personnel*, „Police Crim Psych" 2024, no 39, pp 34–43.

Medical support

All training activities – especially military, police, or firearms-related – must include comprehensive medical coverage to ensure participant safety and rapid response in case of an accident. Medical security includes both appropriate equipment and emergency procedures.[17]

Medical equipment

The instructor issues the command: "Check medical kits – ensure they contain first-aid supplies, dressings, AED defibrillators, and basic medications."

Medical kits should include necessary first-aid items such as dressings, bandages, disinfectants, and AED defibrillators for immediate cardiac response. They should also contain basic medications such as adrenaline, glucagon, or painkillers for emergencies.

Communication with duty officer and emergency numbers

The instructor issues the command: "Ensure constant communication with the duty officer and know emergency numbers – report any incident immediately."

Maintaining contact with the duty officer ensures quick information flow and coordination of rescue actions. Knowing emergency numbers is essential to summon help quickly when needed.

Accident response procedures

The instructor issues the command: "Recall accident response procedures – assess the victim, perform resuscitation, control bleeding, evacuate."

In case of an accident, quick and effective action is essential. The first step is to assess the victim's condition (consciousness and breathing). If necessary, perform cardiopulmonary resuscitation (CPR). For bleeding, immediately apply direct pressure or compression dressings. Evacuation must be carried out safely, following immobilization and transport principles.

First-aid training

Regular first-aid training is necessary to ensure that all participants can provide effective help in emergencies. Such training should cover both theory and practice, including CPR, AED use, bleeding control, and casualty evacuation.

Recommendations for instructors and training leaders

Effective training, especially firearms-related, requires instructors to be well-prepared and continuously improve their competencies. The key recommendations include:

17 A. Martín-Rodríguez, A., Gostian-Ropotin, L. A., Beltrán-Velasco, A. I., Belando-Pedreño, N., Simón, J. A., López-Mora, C., Navarro-Jiménez, E., Tornero-Aguilera, J. F., & Clemente-Suárez, V. J., *Sporting Mind: The Interplay of Physical Activity and Psychological Health*, „Sports" 2024, no 12(1), p 37.

- Thorough preparation of training outlines and equipment lists
  The instructor should carefully plan each part of the training, prepare detailed lesson plans, and list all necessary materials and equipment. Failing to ensure sufficient ammunition, missing magazine tools, or other oversights can cause interruptions and disorganization. Therefore, the principle "better one round too many than one too few" is often emphasized in practice.
- Periodic updating of documentation and procedures
  After each training session, all lesson plans and documentation should be updated and supplemented. This allows instructors to learn from previous experiences, improve procedures, and share best practices with other trainers.
- Training review and debriefing
  After completion, it is essential to analyze the course of training and conduct a debriefing. Instructors should evaluate the effectiveness of their methods, identify organizational and psychophysical issues among participants, and plan corrective actions.
- Experience sharing among instructors
  Regular meetings and exchange of experiences in training techniques and safety practices enhance instructor competence, introduce innovations, and prevent repeating past mistakes.[18]

The instructor should also anticipate potential problems, monitor equipment condition and participant readiness. Organizational consistency of the entire course is as crucial as technical preparation – neglecting either reduces both quality and safety.

Effective training requires careful planning and post-session reflection. Analyzing the course, debriefing, and sharing experience all contribute to continuous improvement of training quality and participant safety.

Summary

Firearms, when handled properly and with respect for safety rules, can be used by individuals of varying experience levels. Modern firearm designs are equipped with safety mechanisms that minimize the risk of accidents and protect both users and bystanders. However, regardless of experience, firearms must always be treated with caution, and all safety procedures must be strictly followed.

An effective safety system for firearms training relies on:

- continuous updating of knowledge and procedures,
- control of equipment and gear condition,
- systematic training for participants and instructors,
- effective planning and post-training analysis.

18 A. Martín-Rodríguez, Gostian-Ropotin at all… p. 37.

Only through consistent application of these principles can training be conducted safely and effectively – developing participant skills while minimizing the risk of incidents and accidents.

Bibliography

Bezpieczeństwo na strzelnicy – podstawowe zasady, Warszawa 2025.

Blalock J.R., Black R.A., Bourke M.L. et al. Emergency Communication Operators: *Findings from the National Wellness Survey for Public Safety Personnel,* „Police Crim Psych" 2024, no 39.

Hemenway D, Rausher S., Violano P., Raybould T., Barber C., *Firearms training: What is actually taught?,* „Injury Prevention" 2017, no 25.

Idzikowski A., *Szkolenie strzeleckie. Bezpieczeństwo – charakterystyka zagadnienia*. Legionowo 2014.

Jha Amishi, Izaguirre Mary & Adler Amy, *Mindfulness Training in Military Settings: Emerging Evidence and Best-Practice Guidance*, „Current Psychiatry Reports" 2025.

Kaczmarski A., *Organizacja systemu szkoleń strzeleckich w polskiej Policji*, „Securitologia" , 2017.

Konopka K., *Prawo i bezpieczeństwo na strzelnicach publicznych*, „Magazyn Policji KSP" 2022.

Martín-Rodríguez A., Gostian-Ropotin L. A., Beltrán-Velasco A. I., Belando-Pedreño N., Simón J. A., López-Mora C., Navarro-Jiménez E., Tornero-Aguilera J. F., & Clemente-Suárez V. J., *Sporting Mind: The Interplay of Physical Activity and Psychological Health,* „Sports" 2024, *no* 12(1).

Ogólne zasady bezpieczeństwa obowiązujące przy uprawianiu sportu strzeleckiego. Polski Związek Strzelectwa Sportowego.

Renner R., Cvetković V. M., & Lieftenegger N., *Dealing with High-Risk Police Activities and Enhancing Safety and Resilience: Qualitative Insights into Austrian Police Operations from a Risk and Group Dynamic Perspective,* „Safety" 2025, no 11(3).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 26 sierpnia 2014 r. w sprawie szczegółowych zasad szkolenia strzeleckiego funkcjonariuszy Policji (Dz.U. 2014 r. poz. 1195).

Ustawa z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz.U. z 2013 r. poz. 628).

Wybrane aspekty bezpieczeństwa podczas zajęć z użyciem broni palnej, Szczytno 2022.

About the Authors

Dominika Grzybowska-Ganszczyk, PhD – is a physiotherapist, medical rescue specialist, and Assistant Professor at the Academy of Physical Education in Katowice, specializing in neurorehabilitation, cardiac rehabilitation, and tactical medicine. Her scientific work includes interdisciplinary research projects conducted in collaboration with biomedical engineering and biomechatronics teams, as well as studies on functional performance and human resilience under physical and environmental

stress. She integrates clinical, academic, and instructional expertise–covering self-defense, intervention tactics, and functional training–to support initiatives relevant to the health and operational safety of uniformed services and the broader society.

Bartosz Głowacki, PhD – is a scholar in physical culture sciences and lecturer at the Jerzy Kukuczka Academy of Physical Education in Katowice, specializing in intervention tactics, self-defence, and operational techniques for uniformed services. His professional background includes extensive instructional and practical experience gained as an educator at the Police School in Katowice, as well as expertise in firearms training, direct coercive measures, tactical interventions, and martial arts, supported by active involvement in sport shooting and advanced tactical training programs. He combines scientific research with operational practice within the Department of Internal Security, contributing to the development of modern training methodologies for law enforcement and special units.

MSc Eng. **Jakub Ganszczyk** is a graduate of the Faculty of Civil Engineering at the Silesian University of Technology and the Faculty of Civil Engineering at Cracow University of Technology, specializing in shooting range infrastructure design. He works at an accredited ballistic laboratory, where he conducts research on the ballistic resistance of materials and protective components. At Works 11 Ltd., he is responsible for the design and implementation of modern shooting range facilities as well as technical consultancy in ballistic safety. His professional activity focuses on developing solutions that enhance the safety and operational efficiency of shooting ranges.

OUR EXPERTS

Patryk Błasik, PhD (WSB University, Poland)

Jarosław Gorzawski, PhD (WSB University, Poland)

Szymon Noworyta, PhD

Gabriela Socha, PhD (Police School in Katowicach, Poland)

Edyta Wcisło, PhD (Regional Blood Donation and Blood Treatment Center in Łódź, Poland)

Oleg Zachko, PhD, Associate Prof. (Lviv State University of Life Safety, Ukraine)

WSB University
Cieplaka 1c 41-300 Dąbrowa Górnicza Poland

www.wsb.edu.pl