Revista JURÍDICA PORTUCALENSE

www.upt.pt

Nº 36 | Universidade Portucalense | Porto | 2024

https://doi.org/10.34625/issn.2183-2705(36)2024

Ihor KHMYROV, Anton KHRIAPYNSKYI, Polina ALIIEVA, Igor KOPOTUN, Ivo SVOBODA

International Experience of Advanced Countries in State Management of Countering Hybrid Threats

DOI: https://doi.org/10.34625/issn.2183-2705(36)2024.ic-16

Secção I

Investigação Científica*

* Os artigos presentes nesta secção foram sujeitos a processo de revisão segundo o método *blind peer review* / The articles in this section have undergone a blind peer review process.

International Experience of Advanced Countries in State Management of Countering Hybrid Threats

Experiência Internacional de Países Avançados na Gestão Estatal de Combate a Ameaças Híbridas

Ihor KHMYROV[1]
Anton KHRIAPYNSKYI[2]
Polina ALIIEVA[3]
Igor KOPOTUN[4]
Ivo SVOBODA[5]

ABSTRACT: Hybrid threats combine various instruments of influence, from traditional military operations to cyberattacks and disinformation activities. These threats severely challenge states' national security and require an adequate response from public authorities. The study examines the experience and the existing approaches of the world's leading countries in the state management of countering hybrid threats. The research methods employed in this study were comprehensive, including a graphical analysis of country profiles, a detailed comparison of international ratings and indices, the basic indicator approach, and an in-depth analysis of strategic documents of individual countries and associations. This comprehensive approach has provided a detailed understanding of the leading countries' main institutional mechanisms, strategies, and measures to counter hybrid warfare, instilling confidence in the study's findings. The study's findings underscore the necessity for an integrated approach to countering hybrid threats and close coordination between different agencies at the national level. The results show that leading countries use specialised structures to coordinate efforts, strengthen cooperation between government agencies and the private and public sectors, implement measures to ensure cybersecurity and protect critical infrastructure, and intensify international cooperation. Recommendations for improving critical infrastructure protection, developing a comprehensive strategy, and strengthening international collaboration are substantiated.
KEYWORDS: hybrid threats; public administration; vulnerability; counteraction; cybersecurity; EU; the USA.

[1] Doctor of Science in Public Administration, Associate Professor, Senior Researcher of Scientific Department of Problems of Civil Protection and Technogenic and Ecological Safety of the Scientific and Research Center, National University of Civil Protection of Ukraine, Kharkiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-7958-463X. E-mail: khmyrovigor08@gmail.com
[2] Candidate of Law, Director of the Khryapinsky and Co., Ltd, Kharkiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-2492-051X. E-mail: khriapynskyi41@gmail.com
[3] Ph.D. of Sciences in Public Administration, Research Associate of Scientific Department of the State Security Problems of Educational-Scientific-Production Center, Kharkiv, Ukraine. ORCID ID: https://orcid.org/0000-0003-2929-1107. E-mail: alin.polya7771@gmail.com
[4] Honored Lawyer of Ukraine, Chief Researcher of Research Laboratory for the Prevention of Criminal Offenses of the Faculty № 3, Donetsk State University of Internal Affairs Kropyvnytskyi, Ukraine. ORCID ID: 0000-0002-2947-8599. E-mail: Igor.kopot1@gmail.com
[5] Associate Professor, Guarantor of Security Management Studies, AMBIS, a.s. Vyská Škola, Praha, Česka Republika. ORCID ID: https://orcid.org/0000-0002-0941-4686. E-mail: svobodaivo985@gmail.com

RESUMO: As ameaças híbridas combinam vários instrumentos de influência, desde operações militares tradicionais até ataques cibernéticos e atividades de desinformação. Estas ameaças desafiam gravemente a segurança nacional dos Estados e exigem uma resposta adequada das autoridades públicas. O estudo examina a experiência e as abordagens existentes dos países líderes mundiais na gestão estatal do combate às ameaças híbridas. Os métodos de investigação utilizados neste estudo foram abrangentes, incluindo uma análise gráfica dos perfis dos países, uma comparação detalhada de classificações e índices internacionais, a abordagem dos indicadores básicos e uma análise aprofundada de documentos estratégicos de países e associações individuais. Esta abordagem abrangente proporcionou uma compreensão detalhada dos principais mecanismos institucionais, estratégias e medidas dos países líderes para combater a guerra híbrida, inspirando confiança nas conclusões do estudo. As conclusões do estudo sublinham a necessidade de uma abordagem integrada para combater as ameaças híbridas e de uma coordenação estreita entre as diferentes agências a nível nacional. Os resultados mostram que os países líderes utilizam estruturas especializadas para coordenar esforços, reforçar a cooperação entre agências governamentais e os sectores público e privado, implementar medidas para garantir a segurança cibernética e proteger infra-estruturas críticas, e intensificar a cooperação internacional.
PALAVRAS CHAVE: ameaças híbridas; administração pública; vulnerabilidade; contra-ação; cíber segurança; UE; Estados Unidos.

1. Introduction

Today's world is characterised by rapid geopolitical transformations and the emergence of new security challenges that require an adequate response from state institutions. One of the key global challenges is hybrid threats, which combine various instruments of pressure - from traditional military operations to cyberattacks, disinformation activities, and economic pressure. Hybrid threats pose a significant challenge to the public administration system, as they require a comprehensive and strategic approach and coordination of efforts of various institutions and bodies.

Ukraine and Western countries were the first to face the manifestations of hybrid warfare, in particular from the Russian Federation. The annexation of Crimea and full-scale military aggression in Ukraine, cyberattacks, propaganda and disinformation have led to a rethinking of approaches to national security and countering hybrid threats. The critical role in this process belongs to the public administration bodies responsible for developing and implementing the relevant policy.

The enemy can use hybrid threats to achieve its goals, combining traditional military means with unconventional approaches such as cyber-attacks, disinformation activities or economic pressure. Effective counteraction to such a

multifaceted threat requires a comprehensive and coordinated use of various resources and capabilities, including diplomacy, military power, intelligence efforts and economic leverage[6].

Studying the international experience of countering hybrid threats is relevant to improving the public administration system, increasing efficiency, and adapting to new security challenges. Studying the best practices of the world's leading countries in this area will allow us to develop recommendations for further strengthening countries' defence capabilities.

The study's main aim is to analyse the experience of the world's leading countries in public administration of countering hybrid threats and formulating recommendations. The main research objectives are as follows:

1. To analyse the threats posed by hybrid conflicts and the challenges encountered by the public administration system.

2. To study the experience of the world's leading countries in countering hybrid threats at the level of public authorities.

3. To identify critical tools and mechanisms countries use to counter hybrid threats.

4. To formulate recommendations for improving the public administration system in countering hybrid threats.

Analysing these issues will allow us to form a comprehensive vision of international practice in countering hybrid threats, identify the most effective approaches and tools, and develop proposals for their implementation in modern state policies to counter existing threats.

2. Literature review

Modern conflicts are increasingly becoming hybrid, where traditional military operations are combined with irregular tactics, decentralised planning, and non-state actors' involvement. Hybrid threats are a multifaceted phenomenon that encompasses the entire spectrum of warfare - from conventional forces to irregular armed groups, terrorist attacks and criminal disorder[7].

[6] DEI, Maryna O., HRYTSAI, Iryna O., DAVYDOVA, Nataliya O. et al. Analysis of the peculiarities of the concept of temporary protection in the Eu in the context of defense against hybrid threats. *Pakistan Journal of Criminology* [online], 2023, vol. 15, n 1, pp. 139-155. Available from: https://www.pjcriminology.com/wp-content/uploads/2023/07/10.-Maryna.-Final-Paper-1.pdf

[7] HOFFMAN, Frank G. Hybrid warfare and challenges. In MAHNKEN, Thomas. G., MAIOLO, Joseph A. *Strategic Studies.* 2nd ed. London: Routledge, 2014, pp. 329-337. ISBN

Hybrid threats are characterised by state and non-state actors using a wide range of nontraditional instruments to gain a strategic advantage in geopolitical confrontation. They can operate below the thresholds of detection and response, using a combination of military, political, economic, and informational measures to destabilise the enemy[8] [9].

These threats exploit vulnerabilities in interconnected human, physical and cyber components, requiring a comprehensive approach to security due to their complex and multidimensional nature. This is manifested in the impact on societies, often going beyond conventional armed conflicts and having profound consequences in various areas[10] [11].

Hybrid threats challenge democratic societies due to their nonlinear and asymmetric nature, involving non-military instruments and civilians as primary targets[12]. Economic interdependence can serve as a distribution channel for hybrid threats, with economically weaker states particularly vulnerable to escalation and manipulation by more powerful actors[13].

Definitions of hybrid threats are diverse, reflecting the ambiguity of the means employed, the forces involved, the geographical areas and the rapid technological changes that shape future conflicts[14]. Hybrid threats can include

9781315814803. Available from: https://www.taylorfrancis.com/chapters/edit/10.4324/9781315814803-24/hybrid-warfare-challenges-frank-hoffman

[8] LUPULESCU, Georgiana Daniela. Hybrid threats-possible consequences in societal contexts. *Proceedings of the 22nd European Conference on Cyber Warfare and Security*, Greece, 2023, vol. 22, n 1, pp. 616-622. https://doi.org/10.34190/eccws.22.1.1119

[9] GÖKCE, O. Definition and scope of hybrid threats. *Inquiry: Critical Thinking Across the Disciplines*, 2017, vol. 3, n 1, pp. 19-30. https://doi.org/10.21533/ISJSS.V3I1.97

[10] RAUGH, David L. Is the hybrid threat a true threat. *Journal of Strategic Security*, 2016, vol. 9, n 2, pp. 1-13. https://doi.org/10.5038/1944-0472.9.2.1507

[11] KRUHLOV, Vitalii, LATYNIN, Mykola, HORBAN, Alina et al. Public-private partnership in cybersecurity. GNATYUK, Sergiy, FEDUSHKO, Solomiia, HU, Zhengbing et al. (Eds.), *International Workshop on Cyber Hygiene CybHyg* [online]. Kyiv: CEUR-WS.org, 2019, pp. 619-628 [viewed 11 July 2024]. Available from: https://er.chdtu.edu.ua/bitstream/ChSTU/3080/1/Digital%20Content%20Processing%20Method%20for%20Biometric%20Identification%20of%20Personality%20Based%20on%20Artificial%20Intelligence%20Approaches.pdf

[12] VALENZA, Fulvio. Next generation of hybrid threats. MEGIAS, D., PIETRO, R. D. (Eds.). In *Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference*. Barcelona: Association for Computing Machinery, 2022, p. 114. ISBN: 978-1-4503-9603-5. https://doi.org/10.1145/3528580.3535333.

[13] KALYUZHNA, N. H., KOVTUN, T. K. Hybrid threats: Essence, characteristics, preconditions for escalation. *The problems of economy*, 2021, vol. 3, n 49, pp. 16-21. https://doi.org/10.32983/2222-0712-2021-3-16-21.

[14] GEORGIANA-DANIELA, Lupulescu. Hybrid – defining the concept of the 21st century warfare, operations and threats. *Bulletin of "Carol I" National Defence University*, 2023, vol. 12, n 2, pp. 56-68. ISSN 2284-9378. https://doi.org/10.53477/2284-9378-23-20.

various actions, such as economic and information pressure, cyber attacks, and the spreading of extremist ideologies that undermine democratic values and the rule of law[15]. These threats are not limited to wartime but increasingly manifest themselves in peacetime, affecting society through fear-induced behavioural changes, migration crises and other challenges. This challenges the foundations of democracy, the rule of law and security, requiring a comprehensive approach to counter their multifaceted impact[16].

In one of the first definitions, a hybrid threat is considered an adversary using "diverse and dynamic combinations of conventional, irregular, terrorist, and criminal capabilities"[17]. It should be noted that in 2023, there was a 22% increase in the number of deaths from terrorism compared to the previous year, and terrorist attacks became more deadly (in 2023, with 2.5 deaths per attack compared to 1.6 in 2022)[18].

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) defines hybrid threats as "methods and actions that target an opponent's vulnerabilities". Vulnerabilities can be created by historical memory, legislation, outdated practices, geostrategic factors, societal polarisation, technological deficiencies or ideological differences[19]. The Ministry of the Interior of the Czech Republic defines hybrid threats as "methods or means used for resistance by military, paramilitary or various civilians"[20]. Galeotti[21] defined hybrid threats as "a style of warfare that combines the political, economic and social in a conflict

[15] CHODAK, Paweł, KRASSOWSKI, Krzysztof, WIERZCHOWSKI, Tomasz. Hybrid threats – means of destabilization of law and order in modern democratics societes. Idea and Methodology of Proposed Research. *Teka Komisji Prawniczej PAN Oddział w Lublinie,* 2022, vol. 14, n 2, pp. 91-100. https://doi.org/10.32084/tekapr.2021.14.2-8

[16] LUPULESCU, Georgiana Daniela. Hybrid threats-possible consequences in societal contexts. *Proceedings of the 22nd European Conference on Cyber Warfare and Security*, Greece*,* 2023, vol. 22, n 1, pp. 616-622. https://doi.org/10.34190/eccws.22.1.1119

[17] CASEY, George W. America's army in an era of persistent conflict. *Army Magazine* [online], 2008, vol. 58, n 10, pp. 19-28. Available from: https://www.ausa.org/sites/default/files/Casey_1008.pdf

[18] Institute for Economics & Peace. "Global peace index 2023: Measuring peace in a complex world" [online]. 10 July 2024. Available from: https://www.visionofhumanity.org/wp-content/uploads/2023/06/GPI-2023-Web.pdf

[19] Hybrid CoE. "Hybrid Threats" [online]. 11 July 2024. Available from: https://www.hybridcoe.fi/hybrid-threats/

[20] Ministerstvo vnitra České republiky. "Co jsou hybridní hrozby?" [online]. 16 July 2024. Available from: https://www.mvcr.cz/cthh/clanek/co-jsou-hybridni-hrozby.aspx

[21] GALEOTTI, Mark. *Hybrid War or Gibridnaya Voina? Getting Russia's non-linear military challenge right.* London: Mayak Intelligence, 2016. ISBN 365549801.

where there are no boundaries between civilians and the military, and achieving victory requires any means to be successful.

Hybrid threats are seen as external threats to national security that require strengthening the legal regulation of the information sphere[22]. Other scholars[23] emphasise that countering these threats depends on establishing legal measures to combat false news and disinformation in cyberspace.

The study[24] examines how aggressors undermine liberal democracies by employing hybrid threats and prepare the ground for full-scale war without open military conflict. States can protect their communities from dangerous actions in a world of global interconnectedness, as well as increase their resilience in the face of new challenges, particularly cyberattacks and disinformation. The relevance of these issues is growing, as modern democracies, despite their military capabilities, remain vulnerable to non-military threats.

Lott[25] examines challenges such as hybrid threats, cyberattacks, piracy, and other forms of aggression that international maritime law and security face. Significant attention is paid to analyzing the legal aspects of maritime security, interaction between states, and the inadequacy of existing legislative frameworks in response to new, complex threats. International cooperation and innovative legal solutions can help states adapt to challenges while maintaining peace and order in global waters[26].

To counter hybrid threats in the cyber sphere, it is necessary to strengthen the legal framework of information policy and promote one's vision of the international order[27]. Analytical studies show that in the current environment, countering hybrid threats and disinformation has become a priority for the

[22] DATZER, Veronika, LONARDO, Luigi. Genesis and evolution of EU anti disinformation policy: Entrepreneurship and political opportunism in regulating digital technology. *Journal of European Integration*, 2022, vol. 45, n 5, pp. 751-766. https://doi.org/10.1080/07036337.2022.2150842
[23] SAURWEIN, Florian, SPENCER-SMITH, Charlotte. Combating disinformation on social media: Multilevel governance and distributed accountability in Europe. *Digital Journalism*, 2020, vol. 8, n 6, pp. 820-841. http://doi.org/10.1080/21670811.2020.1765401
[24] BORCH, Odd Jarl, HEIER, Tormod, Eds. *Preparing for hybrid threats to security: Collaborative preparedness and response.* London, Routledge, 2024. https://doi.org/10.4324/9781032617916
[25] LOTT, Alexander. *Hybrid threats and the Law of the Sea: use of force and discriminatory navigational restrictions in straits*. Leiden, Brill, 2022. https://doi.org/10.1163/9789004509368
[26] LOTT, Alexander. *Hybrid threats and the Law of the Sea: use of force and discriminatory navigational restrictions in straits*. Leiden, Brill, 2022. https://doi.org/10.1163/9789004509368
[27] PEROT, Elie. The art of commitments: NATO, the EU, and the interplay between law and politics within Europe's collective defence architecture. *European Security*, 2019, vol. 28, n 1, pp. 40-65. https://doi.org/10.1080/09662839.2019.1587746.

European Union[2829]. At the same time, when considering EU information legislation through the prism of hybrid threats, experts argue that the primary responsibility of EU member states for countering these threats lies at the national level[30].

Improving information security in the face of hybrid threats requires modernising digital infrastructure to increase its resilience to cyberattacks and external threats, increasing society's digital literacy, and establishing a fair measure of punishment for committing cybercrimes[31].

During hybrid warfare and martial law, the state must protect the national information space from negative information and psychological influences and the harmful effects of digital technologies[32]. To effectively detect and respond to hybrid threats, it is necessary to create systems with internal evaluation mechanisms operating at several levels: individual tools, institutions involved, and the macro level of the entire environment to assess the achievement of common goals[33]. Researchers emphasise the importance of developing a comprehensive strategy to counter hybrid threats at the state level. Such a strategy should cover cybersecurity, countering disinformation, protecting critical infrastructure, and coordination mechanisms between agencies and structures.

The world's leading countries are actively working to improve the public administration system to counter hybrid threats. For example, the Centre for Countering Hybrid Threats (CCHT) is a subdivision of the Institute for Administrative and Security Analyses of the Ministry of the Interior of the Slovak

[28] BAJARŪNAS, Eitvydas. Addressing hybrid threats: Priorities for the EU in 2020 and beyond. *European View*, 2020, vol. 19, n 1, pp. 62-70. ISSN 1865-5831. https://doi.org/10.1177/1781685820912041.
[29] KALNIETE, Sandra, PILDEGOVIČS, Tomass. Strengthening the EU's resilience to hybrid threats. *European View*, 2021, vol. 20, n 1, pp. 23-33. ISSN 1865-5831. https://doi.org/10.1177/17816858211004648.
[30] KHMEL, Anastasiia. Combating hybrid threats in the EU (by the European Union regulation and legal framework). *Acta De Historia & Politica: Saeculum XXI*, 2022, vol. 3, pp. 91-101. ISSN 2786-8788. https://doi.org/10.26693/ahpsxxi2021-2022.03.091
[31] KHRIAPYNSKYI, Anton, KHMYROV, Ihor, SVOBODA, Ivo et al. State information security strategies in conditions of hybrid threats. *Amazonia Investiga*, 2023, vol. 12, n 69, pp. 84-93. ISSN 2322-6307. https://doi.org/10.34069/AI/2023.69.09.7
[32] Zavhorodnia, Yuliia, POVYDYS, Vladyslav, KOZMINYKH, Alona et al. Information policy of the state in the context of growing cyber threats. *Pakistan Journal of Criminology* [online], 2023, vol. 15, n 01, pp. 111-124. Available from: www.pjcriminology.com/wp-content/uploads/2023/07/8.-Yuliia.-Final-Paper.pdf
[33] FILIPEC, Ondrej. Preventing hybrid threats: from identification to an effective response. *European Studies-The Review of European Law, Economics and Politics*, 2021, vol. 8, n 1, pp. 17-38. ISSN 2264-6695. https://doi.org/10.2478/eustu-2022-0063.

Republic[34]. In 2016, the Hybrid Fusion Cell at the European External Action Service was established to monitor and analyse hybrid threats and provide recommendations for policy-making[35]. NATO member states are also actively working to counter hybrid threats. In 2016, the NATO Strategy on Countering Hybrid Warfare was approved[36], providing a comprehensive approach to addressing this issue.

3. Methodology

The research was conducted using a complex methodology, enabling a comprehensive study of the problem and formulating well-founded recommendations.

The methodological approach involves (1) identification of the most significant risks that may affect on a global scale in the coming years; (2) finding out the general state of the countries' capabilities to face modern threats; (3) examining the profiles of individual countries of the world according to the Fragile States Index; (4) finding out, based on the basic indicator approach, trends in terrorist incidents; (5) identifying the main strategic approaches to countering hybrid threats.

To quantitatively assess the effectiveness of measures against hybrid threats, a content analysis of international ratings and indices reflecting the level of cyber security, stability, state protection, counter-terrorism, etc., was conducted. For this purpose, data from such sources as the Global Cybersecurity Index[37], the Fragile States Index[38], the Global Peace Index[39], the Global

[34] Centre for Countering Hybrid Threats. “About us” [online]. 11 July 2024. Available from: https://www.hybridnehrozby.sk/ccht/

[35] BAJARŪNAS, Eitvydas. Addressing hybrid threats: Priorities for the EU in 2020 and beyond. *European View*, 2020, vol. 19, n 1, pp. 62-70. ISSN 1865-5831. https://doi.org/10.1177/1781685820912041

[36] DUCARU, Sorin Dumitry. Framing NATO's approach to hybrid warfare. *Countering Hybrid Threats: Lessons Learned from Ukraine*, 2016, vol. 128, pp. 3-11. https://doi.org/10.3233/978-1-61499-651-4-3.

[37] E-GA. “National Cyber Security Index” [online]. 11 July 2024. Available from: https://ncsi.ega.ee/ncsi-index/?order=rank

[38] Fund for Peace. “Fragile states index annual report 2023” [online]. 11 July 2024. Available from: https://fragilestatesindex.org/wp-content/uploads/2023/06/FSI-2023-Report_final.pdf

[39] Institute for Economics & Peace. “Global terrorism index 2024: Measuring the impact of terrorism”. [online]. 11 July 2024. Available from: https://www.visionofhumanity.org/wp-content/uploads/2024/02/GTI-2024-web-290224.pdf.

Terrorism Index[40] and the European Union Agency for Law Enforcement Cooperation[41] were used.

The Fragile States Index is an indicator of countries worldwide based on the various pressures they face, affecting their fragility level. The index includes the Security Apparatus Indicator, which considers multiple hybrid threats to state security (attacks, uprisings, coups, terrorism, and private armed groups). A lower indicator value means a more stable position in the country[42]. The Global Peace Index assesses states' relative level of peacefulness by analysing internal and external conflicts and the level of crime and militarization. Higher values indicate lower peacefulness[43]. The Global Terrorism Index reflects global trends and the impact of terrorism on specific countries or regions. Higher values indicate more excellent activity of terrorist groups[44].

The final stage included an analysis of the relevant regulations, strategies and programmes in place in the United States of America, the European Union, and NATO member states facing hybrid warfare. Particular attention was paid to institutional mechanisms and structures to coordinate efforts in this area.

Based on the results obtained, recommendations for improving the public administration system in countering hybrid threats were formulated.

4. Results

Studying general threats to modern countries involves identifying the most significant risks that may be faced shortly (usually, the horizon is between 1 and 10 years). From the general array, it is necessary to single out the areas under study, that is, adverse events that may arise due to hybrid threats and manifestations by various actors.

[40] Institute for Economics & Peace. “Global peace index 2023: Measuring peace in a complex world” [online]. 10 July 2024. Available from: https://www.visionofhumanity.org/wp-content/uploads/2023/06/GPI-2023-Web.pdf
[41] Europol. “EU terrorism situation & trend report (TE-SAT)” [online]. 11 July 2024. Available from: https://www.europol.europa.eu/publications-events/main-reports/tesat-report
[42] Fund for Peace. “Fragile states index annual report 2023” [online]. 11 July 2024. Available from: https://fragilestatesindex.org/wp-content/uploads/2023/06/FSI-2023-Report_final.pdf
[43] Institute for Economics & Peace. “Global terrorism index 2024: Measuring the impact of terrorism”. [online]. 11 July 2024. Available from: https://www.visionofhumanity.org/wp-content/uploads/2024/02/GTI-2024-web-290224.pdf
[44] Institute for Economics & Peace. “Global peace index 2023: Measuring peace in a complex world” [online]. 10 July 2024. Available from: https://www.visionofhumanity.org/wp-content/uploads/2023/06/GPI-2023-Web.pdf

The Global Risks Report 2024 results highlight current crises that undermine resilience and may result from hybrid conflict, as well as new and rapidly evolving sources of risk that may manifest themselves in the coming years (Figure 1). The data in Fig. 1 shows that the most significant risks are related to information security and socio-political issues, reflecting current global trends where technological threats and social divisions are becoming essential risk factors. The correlation indicates that states increasingly face problems not only from conventional military threats, but also from widespread non-military threats such as cyberattacks, disinformation, and economic coercion. This highlights the need for a multifaceted approach that combines cybersecurity, state policy, and cross-sector cooperation to effectively counter these emerging risks.

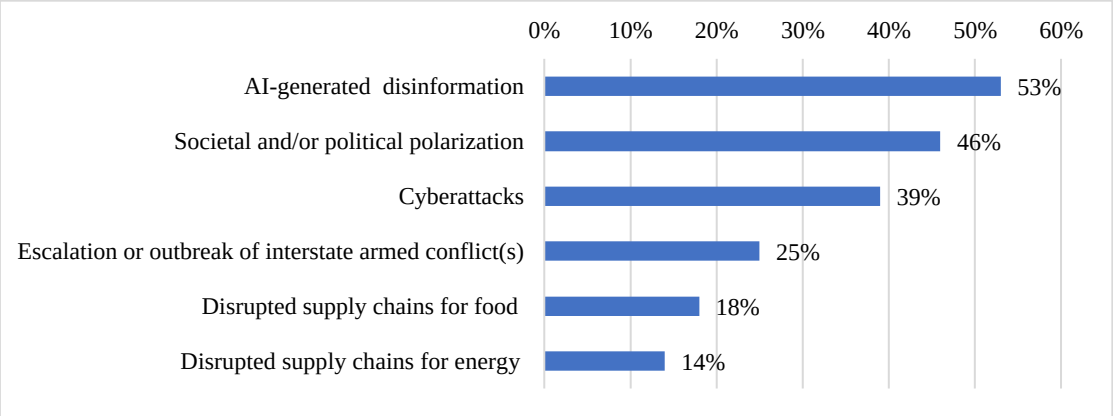

Figure 1 – The most significant risks may affect the global economy in the coming years. Developed by the authors based on World economic forum[45]

To find out the general ability of countries to resist modern threats, we will consider the indicators of the Fragile States Index, which determines the general ability to withstand various threats, including hybrid threats to the security of the state (Fig. 2). This data demonstrates that the Nordic countries (Norway, Iceland, Finland) are the less fragile with the lowest scores, taking into account various factors, including political stability, economic performance and social conditions.

[45] World economic forum. "Global Risks Report 2024" [online]. 11 July 2024. Available from: https://www.weforum.org/publications/global-risks-report-2024/

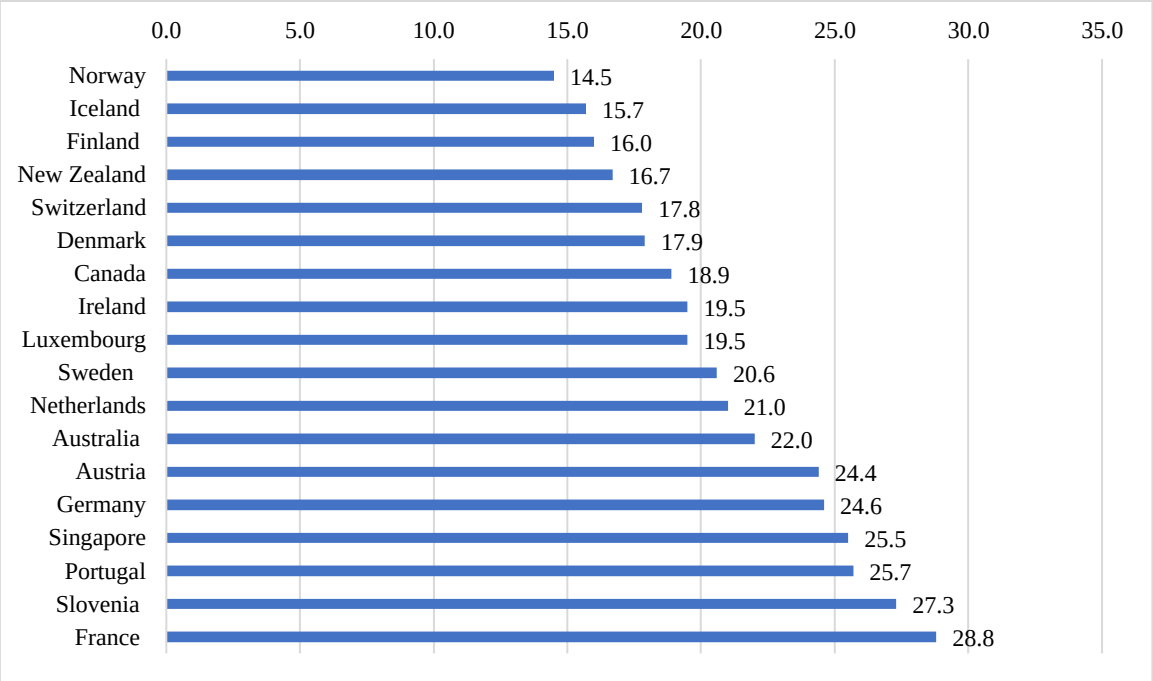

Figure 2 – Indicators of the leading countries in the Fragile States Index, 2023 Compiled by the authors based on Fund for Peace[46]

Let's focus on the profiles of the USA, UK, France, Norway, and Germany. The essential components of the calculation include the Security Apparatus Indicator (threats to state security, including hybrid ones), Factionalized Elites Indicator (fragmentation of state institutions on various grounds and confrontation between elites), Group Grievance Indicator (splits between different groups in society); External Intervention Indicator (influence of external actors on the functioning of the state) (Fig. 3)[47].

According to Fig. 3, Norway's scores in all categories indicate its stability as a state. Germany, France and the UK have moderate values in the 1-3 points range. At the same time, the United States demonstrates the highest scores among these countries in three categories: factionalised elites, group grievances, and external intervention, which is close to 6-7 points. This indicates deep societal differences that make them more susceptible to hybrid threats. The diagram shows the relative level of stability or fragility of the surveyed developed countries according to the Index, indicating certain problem areas in the countries.

[46] Fund for Peace. “Fragile states index annual report 2023” [online]. 11 July 2024. Available from: https://fragilestatesindex.org/wp-content/uploads/2023/06/FSI-2023-Report_final.pdf
[47] Fund for Peace. “Fragile states index annual report 2023” [online]. 11 July 2024. Available from: https://fragilestatesindex.org/wp-content/uploads/2023/06/FSI-2023-Report_final.pdf

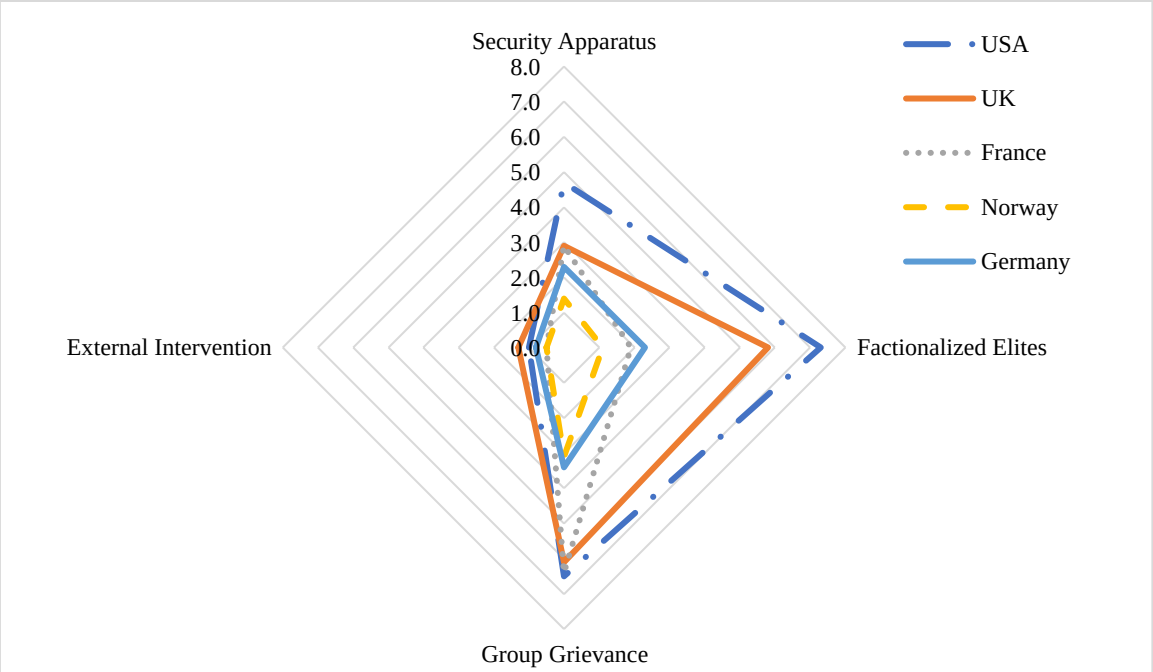

Figure 3 – Profiles of individual countries according to the Fragile States Index, 2023. Developed by the authors based on Fund for Peace[48]

Another approach, based on the Global Peace Index and the Global Terrorism Index, determines countries' problem areas and the possibility of hybrid threats. Let us consider the indicators of some developed countries (Fig. 4).

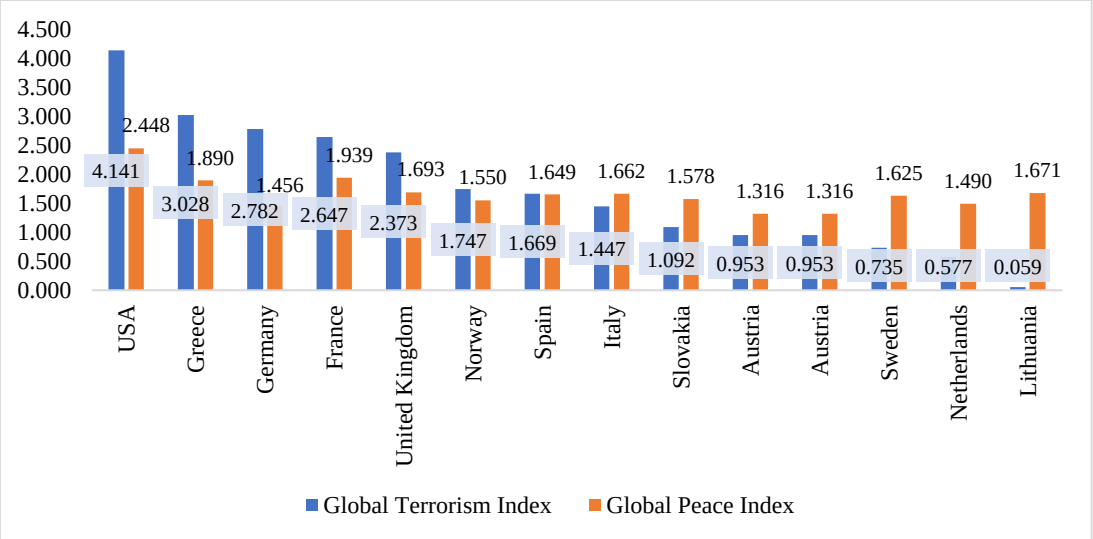

Figure 4 – Indicators of the Global Peace Index and the Global Terrorism Index. Developed by the authors[49] [50].

[48] Fund for Peace. "Fragile states index annual report 2023" [online]. 11 July 2024. Available from: https://fragilestatesindex.org/wp-content/uploads/2023/06/FSI-2023-Report_final.pdf

[49] Institute for Economics & Peace. "Global terrorism index 2024: Measuring the impact of terrorism". [online]. 11 July 2024. Available from: https://www.visionofhumanity.org/wp-content/uploads/2024/02/GTI-2024-web-290224.pdf

[50] Institute for Economics & Peace. "Global peace index 2023: Measuring peace in a complex world" [online]. 10 July 2024. Available from: https://www.visionofhumanity.org/wp-content/uploads/2023/06/GPI-2023-Web.pdf

These charts allow us to compare the situation with terrorism and the overall level of peace in developed countries, identify problem areas and better understand security challenges. The USA has the highest Global Terrorism Index score among the countries represented, while Greece and Germany also have high values. At the same time, Norway, Spain, Italy, Slovakia, and Austria have relatively low global terrorism scores. As for the Global Peace Index, the USA also tops the list. Greece, Germany and France also have relatively high scores. Lithuania, the Netherlands and Austria have the lowest Global Peace Index scores, reflecting the low levels of internal and external conflict, crime and militarisation in these countries. This comparative analysis provides important information about the strengths and weaknesses of each country, emphasizing the importance of adapted, proactive governance strategies to counter hybrid threats and promote resilience in diverse socio-political environments. An analysis of empirical data on terrorist activity in the EU shows that in the period 2018-2022, more than 200 terrorist acts were committed in Europe[51], which caused severe consequences (Table 1). The baseline indicators demonstrate the dynamics over five years relative to the baseline period (2018). The most significant increase in terrorist acts was in Spain, Belgium, and Germany. Despite the overall decrease in incidents in some European countries in 2022, there was an increase in the number of terrorist attacks over 2018-2022.

Table 1 – Terrorist attacks in the EU in 2018-2022

EU Member State	2018	2019	2020	2021	2022	Total for five years (% increase)	Trends (2022 compared to 2018)
Belgium	1	1	2	1	3	8 (700)	+2
France	30	7	15	5	6	63 (110)	-24
Germany	2	3	6	3	1	15 (650)	-1
Greece	7	4	-		4	15 (114,3)	-3
Italy	13	28	24	-	12	78 (500)	-1
Netherlands	4	2	-	-	-	6 (50)	-4
Spain	1	3	9	1	1	15 (1400)	0
Sweden	1	-		2	-	3 (200)	+1
Total	59	48	56	12	27	202 (242,4)	-32

Compiled and calculated by the authors based on Europol[52].

[51] Europol. “EU terrorism situation & trend report (TE-SAT)” [online]. 11 July 2024. Available from: https://www.europol.europa.eu/publications-events/main-reports/tesat-report

[52] Europol. “EU terrorism situation & trend report (TE-SAT)” [online]. 11 July 2024. Available from: https://www.europol.europa.eu/publications-events/main-reports/tesat-report

Based on the general state of affairs, the experience of the world's leading countries shows a variety of approaches and tools used to counter hybrid threats at the level of state authorities. Among the key ones is creating specialised structures and centres to coordinate efforts in countering hybrid threats, such as the Hybrid Fusion Cell in the EU, the Hybrid CoE, etc.

Strengthening cooperation between government agencies, the private sector, and non-governmental organisations in countering hybrid threats involves exchanging information, conducting joint exercises, and developing security guidelines and standards. It should be based on exchanging information and experience and developing common standards and protocols for responding to hybrid threats.

To quantitatively assess the effectiveness of countermeasures against hybrid threats, international ratings and indices reflecting the level of cyber security were analysed. According to the National Cyber Security Index, calculated by the International Telecommunication Union, the leaders in cybersecurity are the USA, the UK, France, Lithuania, and Estonia (Fig. 5).

Fig. 5 shows the leaders in ensuring a secure cyberspace and countering cyber threats as an element of hybrid threats, where high scores indicate solid cyber defence capabilities, effective security strategies, and policies of these states. The Czech Republic is at the top of the ranking, indicating a very high level of cybersecurity. Ukraine ranks 7th, together with Slovakia, meaning it has a relatively strong cybersecurity position.

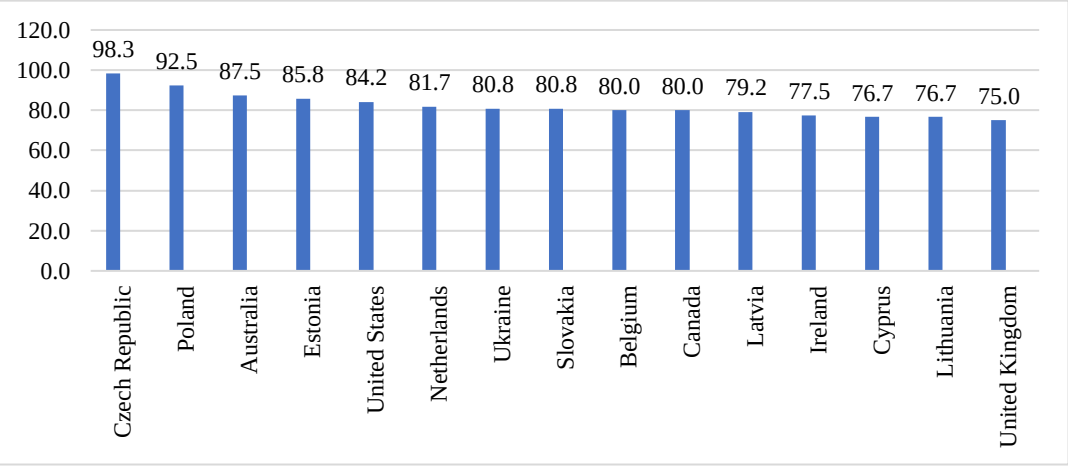

Figure 5 – Indicators of the Top 15 countries according to the National Cybersecurity Index, 2024. Developed by the authors based on E-GA[53]

[53] E-GA. "National Cyber Security Index" [online]. 11 July 2024. Available from: https://ncsi.ega.ee/ncsi-index/?order=rank

Countering hybrid threats by ensuring cybersecurity and protecting critical infrastructure from cyberattacks and other destructive influences involves the following measures: creating specialised cyber defence units, conducting regular security audits of information systems, implementing security standards, and training highly qualified personnel in cybersecurity. An analysis of international practice in countering hybrid threats has revealed several practical tools and mechanisms used by the world's leading countries at the level of government. Leading countries develop strategic documents that define priority areas of activity, distribute powers between agencies and provide mechanisms for their interaction (Table 2).

Table 2 – Strategies for Countering Hybrid Threats

Country, association	Strategy	Key points
USA	The National Security Strategy	The US National Security Strategy lists national security challenges and ways to address them[54].
EU	EU Global Strategy	Europe is protected through crisis management, border protection, and efforts to combat extremism, cyber-attacks, and disinformation through the 'nexus' between internal and external security[55].
EU	EU's Cybersecurity Strategy for the Digital Decade.	Provides for the establishment of the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe) to support the coordinated management of large-scale cybersecurity incidents and crises at the operational level and ensure regular information exchange between Member States and EU institutions, bodies, offices and agencies[56].
EU	The Strategic Compass of the European Union	The Strategic Compass provides a joint assessment of threats and challenges and the strategic environment in which the EU operates. Actionable proposals with a timetable for implementation have been identified to improve the EU's ability to protect its security and citizens. Emphasis is placed on action, investment, partnership, and security[57].

[54] White House. "National security strategy of the United States of America" [online]. 22 October 2022. Available from: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

[55] European Commission. "Communication from the commission to the European Parliament, the council, the European economic and social committee and the committee of the regions. 2016 Communication on EU Enlargement Policy" [online]. 10 July 2024. Available from: https://www.eeas.europa.eu/sites/default/files/20161109_strategy_paper_en.pdf

[56] Council of the European Union. "EU Cyber Defence Policy Framework" [online]. 11 July 2024. Available from: https://ccdcoe.org/uploads/2018/11/EU-141118-EUCyberDefencePolicyFrame-2.pdf

[57] European Union. "A strategic compass for security and defence" [online]. 12 July 2024. Available from: https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

These strategies provide a comprehensive and coordinated approach to countering hybrid threats at the state level and create a basis for developing sectoral programmes and action plans.

Effective countering hybrid threats requires close cooperation between various stakeholders. Leading countries actively engage the private sector, particularly information technology and cybersecurity companies, in developing measures to protect against cyberattacks and disinformation activities. In addition, considerable attention is paid to raising public awareness of hybrid threats and building society's resilience to destructive influences. For this purpose, information campaigns, digital literacy training, and training programmes for various target audiences are being conducted.

The results demonstrate the complex nature of the measures taken by the world's leading countries to counter hybrid threats at the level of government authorities. The measures cover various areas, from ensuring cybersecurity and protecting critical infrastructure to building society's resilience to destructive influences and strengthening international cooperation.

5. Discussion

The results of the study presented in this article confirm the urgency of the problem of countering hybrid threats and the need to improve the relevant mechanisms at the level of public administration. This is consistent with the conclusions of many scholars and experts in this field.

Many researchers dwell on the complex nature of hybrid threats, which combine various modes of warfare, including conventional means, irregular tactics, terrorist acts and criminal acts[58]. It is noted that hybrid threats require the coordinated use of all available resources, including political, military, intelligence, and economic. This is consistent with the position of other scholars who emphasise the need to develop a comprehensive strategy to counter hybrid threats at the state level.

[58] WEISSMANN, Mikael, NILSSON, Niklas, PALMERTZ, Bjorn et al. Conceptualizing and countering hybrid threats and hybrid warfare: The role of the military in the grey zone. In *Hybrid warfare: Security and asymmetric conflict in international relations*. London: I. B. Tauris, 2021, pp. 61-82. ISBN 978-1-7883-1779-5. http://dx.doi.org/10.5040/9781788317795.0011

The study results confirm the importance of creating specialised structures and centres to coordinate efforts to counter hybrid threats. Other scholars[59] also make similar recommendations, emphasising the need for internal mechanisms to assess the effectiveness of measures to counter hybrid threats. Attention is also drawn to the need to strengthen cooperation between government agencies, the private sector, and non-governmental organisations in countering hybrid threats.

Researchers see cybersecurity as a critical aspect of countering hybrid threats and emphasise the importance of ensuring cybersecurity and protecting critical infrastructure from cyberattacks and other destructive influences[60], [61].

The study results confirm the need to strengthen international cooperation and coordinate efforts to counter hybrid threats. This position is supported by many experts who emphasise the transnational nature of hybrid threats and the importance of sharing information and experience and developing common standards[62].

The following recommendations can be made to improve the public administration's system for countering hybrid threats.

1. Develop a national strategy for countering hybrid threats that will identify priority areas of activity, distribute powers between authorities and provide mechanisms for their interaction.

2. Create a unified platform for protection against cyber threats and disinformation that brings together government agencies, private companies, civil society organizations, and academia. Such a platform will enable operational information exchange, coordination of actions during crisis situations, and facilitate the integration of new analytical tools for identifying sources of disinformation and rapid response to threats.

---

[59] FILIPEC, Ondrej. Multilevel analysis of the 2021 Poland-Belarus border crisis in the context of hybrid threats. *Central European Journal of Politics*, 2022, vol. 8, n 1, pp. 1-18. https://doi.org/10.24132/cejop_2022_1

[60] LONARDO, Luigi. EU law against hybrid threats: A first assessment. European Papers. *A Journal on Law and Integration*, 2021, vol. 6, n 2, pp. 1075-1096. ISSN 2499-8249. https://doi.org/10.15166/2499-8249/514

[61] SAURWEIN, Florian, SPENCER-SMITH, Charlotte. Combating disinformation on social media: Multilevel governance and distributed accountability in Europe. *Digital Journalism*, 2020, vol. 8, n 6, pp. 820-841. http://doi.org/10.1080/21670811.2020.1765401

[62] KALNIETE, Sandra, PILDEGOVIČS, Tomass. Strengthening the EU's resilience to hybrid threats. *European View*, 2021, vol. 20, n 1, pp. 23-33. ISSN 1865-5831. https://doi.org/10.1177/17816858211004648

3. Implementation of risk forecasting tools based on monitoring of current data that signal possible increase in risks, such as growth in terrorist activity or disinformation attacks, which will allow early detection of potential threats and vulnerabilities. The use of indices (such as the Global Cyber Vulnerability Index and International Resilience Index) will enable prompt policy adjustments and ensure flexible response to emerging challenges, which is crucial for countries prone to frequent information attacks and cyber incidents.

4. Intensify international cooperation and coordination of efforts in countering hybrid threats, focusing on intelligence sharing, joint exercises, and developing common standards and response protocols.

5. Strengthen critical infrastructure protection from cyber-attacks through regular security audits, implementing cybersecurity standards, training highly qualified specialists, and creating specialised cyber defence units.

Implementation of the recommendations will help increase the efficiency of the public administration system in countering hybrid threats, ensure the coordination of efforts of various agencies, and strengthen national security.

6. Conclusions

Hybrid threats pose a complex challenge in modern conflicts. They are characterised by their hidden nature, different methods, and ability to exploit interconnected vulnerabilities in human, physical, and cyber environments. The world's leading countries are actively working to improve the public administration system to counter hybrid threats. Specialised structures and centres are being created to coordinate efforts, strategies and concepts are being developed, cooperation between various stakeholders is being strengthened, and measures are being taken to ensure cybersecurity, protect critical infrastructure, and combat disinformation.

Ensuring cybersecurity and protecting critical infrastructure from cyberattacks and other destructive influences are priority areas for the world's leading countries in countering hybrid threats. Creating specialised cyber defence units, regular security audits, and developing and implementing security standards help increase countries' resilience to hybrid threats.

International cooperation and coordination of efforts are crucial in countering hybrid threats, often transnational. Sharing information and

experience, coordinating efforts, conducting joint exercises, and developing common standards within international organisations such as the UN, NATO, and the EU allow us to counter the challenges of hybrid warfare more effectively.

It is strongly advisable to conduct constant monitoring and analysis of hybrid threats, engage experts in relevant fields, improve the legal framework governing countering hybrid threats, and raise public awareness of hybrid threats and methods of neutralising them, which will help build society's resilience to destructive influences. In the future, an integrated and coordinated approach at all levels of government will allow the effective countering of hybrid threats and strengthening of national security. The future research direction may be an analysis of approaches to forming strategies for preventive counteraction to hybrid threats.

REFERENCES

BAJARŪNAS, Eitvydas. Addressing hybrid threats: Priorities for the EU in 2020 and beyond. *European View*, 2020, vol. 19, n 1, pp. 62-70. ISSN 1865-5831. https://doi.org/10.1177/1781685820912041.

BORCH, Odd Jarl, HEIER, Tormod, Eds. *Preparing for hybrid threats to security: Collaborative preparedness and response*. London, Routledge, 2024. ISBN 9781032617916. https://doi.org/10.4324/9781032617916

CASEY, George W. America‘s army in an era of persistent conflict. *Army Magazine* [online], 2008, vol. 58, n 10, pp. 19-28. Available from: https://www.ausa.org/sites/default/files/Casey_1008.pdf

Centre for Countering Hybrid Threats. “About us” [online]. 11 July 2024. Available from: https://www.hybridnehrozby.sk/ccht/

CHODAK, Paweł, KRASSOWSKI, Krzysztof, WIERZCHOWSKI, Tomasz. Hybrid threats – means of destabilization of law and order in modern democratics societes. Idea and Methodology of Proposed Research. *Teka Komisji Prawniczej PAN Oddział w Lublinie,* 2022, vol. 14, n 2, pp. 91-100. https://doi.org/10.32084/tekapr.2021.14.2-8

Council of the European Union. “EU Cyber Defence Policy Framework” [online]. 11 July 2024. Available from: https://ccdcoe.org/uploads/2018/11/EU-141118-EUCyberDefencePolicyFrame-2.pdf

DATZER, Veronika, LONARDO, Luigi. Genesis and evolution of EU anti disinformation policy: Entrepreneurship and political opportunism in regulating digital technology. *Journal of European Integration*, 2022, vol. 45, n 5, pp. 751-766. https://doi.org/10.1080/07036337.2022.2150842

DEI, Maryna O., HRYTSAI, Iryna O., DAVYDOVA, Nataliya O. et al. Analysis of the peculiarities of the concept of temporary protection in the Eu in the context of defense

against hybrid threats. *Pakistan Journal of Criminology* [online], 2023, vol. 15, n 1, pp. 139-155. Available from: https://www.pjcriminology.com/wp-content/uploads/2023/07/10.-Maryna.-Final-Paper-1.pdf

DUCARU, Sorin Dumitry. Framing NATO's approach to hybrid warfare. *Countering Hybrid Threats: Lessons Learned from Ukraine*, 2016, vol. 128, pp. 3-11. https://doi.org/10.3233/978-1-61499-651-4-3

E-GA. "National Cyber Security Index" [online]. 11 July 2024. Available from: https://ncsi.ega.ee/ncsi-index/?order=rank

European Commission. "Communication from the commission to the European Parliament, the council, the European economic and social committee and the committee of the regions. 2016 Communication on EU Enlargement Policy" [online]. 10 July 2024. Available from: https://www.eeas.europa.eu/sites/default/files/20161109_strategy_paper_en.pdf

European Union. "A strategic compass for security and defence" [online]. 12 July 2024. Available from: https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

Europol. "EU terrorism situation & trend report (TE-SAT)" [online]. 11 July 2024. Available from: https://www.europol.europa.eu/publications-events/main-reports/tesat-report

FILIPEC, Ondrej. Preventing hybrid threats: from identification to an effective response. *European Studies-The Review of European Law, Economics and Politics*, 2021, vol. 8, n 1, pp. 17-38. ISSN 2264-6695. https://doi.org/10.2478/eustu-2022-0063

FILIPEC, Ondrej. Multilevel analysis of the 2021 Poland-Belarus border crisis in the context of hybrid threats. *Central European Journal of Politics*, 2022, vol. 8, n 1, pp. 1-18. https://doi.org/10.24132/cejop_2022_1

Fund for Peace. "Fragile states index annual report 2023" [online]. 11 July 2024. Available from: https://fragilestatesindex.org/wp-content/uploads/2023/06/FSI-2023-Report_final.pdf

GALEOTTI, Mark. *Hybrid War or Gibridnaya Voina? Getting Russia's non-linear military challenge right.* London: Mayak Intelligence, 2016. ISBN 365549801.

GEORGIANA-DANIELA, Lupulescu. Hybrid – defining the concept of the 21st century warfare, operations and threats. *Bulletin of "Carol I" National Defence University*, 2023, vol. 12, n 2, pp. 56-68. ISSN 2284-9378. https://doi.org/10.53477/2284-9378-23-20

GIANNOPOULOS, G., SMITH, H., THEOCHARIDOU, M. *The landscape of hybrid threats: A conceptual model*. Ispra: Publications Office of the European Union, 2021. ISBN 978-92-76-29819-9. https://doi.org/10.2760/44985

GÖKCE, O. Definition and scope of hybrid threats. *Inquiry: Critical Thinking Across the Disciplines*, 2017, vol. 3, n 1, pp. 19-30. https://doi.org/10.21533/ISJSS.V3I1.97

HOFFMAN, Frank G. Hybrid warfare and challenges. In MAHNKEN, Thomas. G., MAIOLO, Joseph A. *Strategic Studies.* 2nd ed. London: Routledge, 2014, pp. 329-337. ISBN 9781315814803. Available from:

https://www.taylorfrancis.com/chapters/edit/10.4324/9781315814803-24/hybrid-warfare-challenges-frank-hoffman

Hybrid CoE. "Hybrid Threats" [online]. 11 July 2024. Available from: https://www.hybridcoe.fi/hybrid-threats/

Institute for Economics & Peace. "Global peace index 2023: Measuring peace in a complex world" [online]. 10 July 2024. Available from: https://www.visionofhumanity.org/wp-content/uploads/2023/06/GPI-2023-Web.pdf

Institute for Economics & Peace. "Global terrorism index 2024: Measuring the impact of terrorism". [online]. 11 July 2024. Available from: https://www.visionofhumanity.org/wp-content/uploads/2024/02/GTI-2024-web-290224.pdf

KALNIETE, Sandra, PILDEGOVIČS, Tomass. Strengthening the EU's resilience to hybrid threats. *European View*, 2021, vol. 20, n 1, pp. 23-33. ISSN 1865-5831. https://doi.org/10.1177/17816858211004648

KALYUZHNA, N. H., KOVTUN, T. K. Hybrid threats: Essence, characteristics, preconditions for escalation. *The problems of economy*, 2021, vol. 3, n 49, pp. 16-21. https://doi.org/10.32983/2222-0712-2021-3-16-21

KHMEL, Anastasiia. Combating hybrid threats in the EU (by the European Union regulation and legal framework). *Acta De Historia & Politica: Saeculum XXI*, 2022, vol. 3, pp. 91-101. ISSN 2786-8788. https://doi.org/10.26693/ahpsxxi2021-2022.03.091

KHRIAPYNSKYI, Anton, KHMYROV, Ihor, SVOBODA, Ivo et al. State information security strategies in conditions of hybrid threats. *Amazonia Investiga*, 2023, vol. 12, n 69, pp. 84-93. ISSN 2322-6307. https://doi.org/10.34069/AI/2023.69.09.7

KRUHLOV, Vitalii, LATYNIN, Mykola, HORBAN, Alina et al. Public-private partnership in cybersecurity. GNATYUK, Sergiy, FEDUSHKO, Solomiia, HU, Zhengbing et al. (Eds.), *International Workshop on Cyber Hygiene CybHyg* [online]. Kyiv: CEUR-WS.org, 2019, pp. 619-628 [viewed 11 July 2024]. Available from: https://er.chdtu.edu.ua/bitstream/ChSTU/3080/1/Digital%20Content%20Processing%20Method%20for%20Biometric%20Identification%20of%20Personality%20Based%20on%20Artificial%20Intelligence%20Approaches.pdf

LONARDO, Luigi. EU law against hybrid threats: A first assessment. European Papers. *A Journal on Law and Integration*, 2021, vol. 6, n 2, pp. 1075-1096. ISSN 2499-8249. https://doi.org/10.15166/2499-8249/514

LOTT, Alexander. *Hybrid threats and the Law of the Sea: use of force and discriminatory navigational restrictions in straits.* Leiden, Brill, 2022. ISBN 9789004509351 https://doi.org/10.1163/9789004509368

LUPULESCU, Georgiana Daniela. Hybrid threats-possible consequences in societal contexts. *Proceedings of the 22nd European Conference on Cyber Warfare and Security*, Greece, 2023, vol. 22, n 1, pp. 616-622. https://doi.org/10.34190/eccws.22.1.1119

Ministerstvo vnitra České republiky. "Co jsou hybridní hrozby?" [online]. 16 July 2024. Available from: https://www.mvcr.cz/cthh/clanek/co-jsou-hybridni-hrozby.aspx

PEROT, Elie. The art of commitments: NATO, the EU, and the interplay between law and politics within Europe's collective defence architecture. *European Security*, 2019, vol. 28, n 1, pp. 40-65. https://doi.org/10.1080/09662839.2019.1587746

RAUGH, David L. Is the hybrid threat a true threat. *Journal of Strategic Security*, 2016, vol. 9, n 2, pp. 1-13. https://doi.org/10.5038/1944-0472.9.2.1507

SAURWEIN, Florian, SPENCER-SMITH, Charlotte. Combating disinformation on social media: Multilevel governance and distributed accountability in Europe. *Digital Journalism*, 2020, vol. 8, n 6, pp. 820-841. http://doi.org/10.1080/21670811.2020.1765401

VALENZA, Fulvio. Next generation of hybrid threats. MEGIAS, D., PIETRO, R. D. (Eds.). In *Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference*. Barcelona: Association for Computing Machinery, 2022, p. 114. ISBN: 978-1-4503-9603-5. https://doi.org/10.1145/3528580.3535333

WEISSMANN, Mikael, NILSSON, Niklas, PALMERTZ, Bjorn et al. Conceptualizing and countering hybrid threats and hybrid warfare: The role of the military in the grey zone. In *Hybrid warfare: Security and asymmetric conflict in international relations*. London: I. B. Tauris, 2021, pp. 61-82. ISBN 978-1-7883-1779-5. http://dx.doi.org/10.5040/9781788317795.0011

White House. "National security strategy of the United States of America" [online]. 22 October 2022. Available from: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

World economic forum. "Global Risks Report 2024" [online]. 11 July 2024. Available from: https://www.weforum.org/publications/global-risks-report-2024/

Zavhorodnia, Yuliia, POVYDYS, Vladyslav, KOZMINYKH, Alona et al. Information policy of the state in the context of growing cyber threats. *Pakistan Journal of Criminology* [online], 2023, vol. 15, n 01, pp. 111-124. Available from: www.pjcriminology.com/wp-content/uploads/2023/07/8.-Yuliia.-Final-Paper.pdf

Data de submissão do artigo: 18/07/2024

Data de aprovação do artigo: 01/11/2024

Edição e propriedade:
Universidade Portucalense Cooperativa de Ensino Superior, CRL
Rua Dr. António Bernardino de Almeida, 541 - 4200-072 Porto
Email: upt@upt.pt