Pakistan Journal of Criminology
Vol. 16, No. 03, July—September 2024 (1037-1052)

The Role of Public Administration in Countering Hybrid Threats in Cyberspace

Anton Khriapynskyi[1], Ihor Khmyrov[2], Polina Aliieva[3],
Borys Dziundziuk[4] & Ivo Svoboda[5]

Abstract

The study aims to evaluate the involvement of public administration in addressing hybrid threats in cyberspace. A comparative analysis was conducted on the entities involved in combating hybrid threats in the digital realm in Ukraine, France, and Japan, utilising visual and graphic techniques. It was established that the prevalence of hybrid threats targeting the cyber domain is contingent upon adequate organisational support. The subjects of public administration in countering hybrid threats in cyberspace in Ukraine, France and Japan were indicated. It was determined that hybrid threats predominantly encompass challenges to a state's sovereignty, national security, public awareness, classified information, and communication. It is important to acknowledge many constantly evolving tactics and strategies employed in these threats. At the same time, there is potential to draw upon the experience of France and Japan and establish a separate entity in Ukraine dedicated to countering hybrid threats in cyberspace. Future research could explore the feasibility of implementing such a system in Ukraine, highlighting the key tasks, goals, competencies, authorities, functions, and operational objectives.

Keywords: public administration, hybrid threats, cyberspace, cyberattacks, national security, blockchain.

Introduction

Globalisation changes, rapid scientific and technological development and the introduction of digitalisation in all spheres of public life are characteristics of the modern information society. The advancement of states towards technology fosters the creation of myriad new possibilities (Bradshaw & Howard, 2019).

[1]The author works at the Khryapinsky and Co., Ltd., Ukraine. antonhrapinsk@gmail.com
[2]The author works at the 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, Ukraine. khmyrov7451@gmail.com
[3]The author works at the Scientific Department of the State Security Problems of Educational-Scientific-Production Center, National University of Civil Defence of Ukraine, Ukraine. polyapoli@gmail.com
[4]The author works at the Department of Law, National Security and European Integration, Education and Scientific Institute "Institute of Public Administration", V.N. Karazin Kharkiv National University, Ukraine. zhandassofen@gmail.com
[5]The author works at AMBIS, a.s. Vyská škola, Czech Republic. Svoboda.Ivo64@seznam.cz

However, such development is accompanied by new challenges and threats, particularly in the security sphere, both at the national and international levels.

It should be noted that the role of state administration in countering hybrid threats in cyberspace is to implement a set of measures to monitor information and communication systems. This is the implementation of control over compliance with standards in the field of information security and the detection of cyber spies who are trying to hack into appropriate assets and possess trade secrets (NATO, 2021).

Cyberspace and other physical spaces are recognised as one of the possible theatres of war. The trend towards the creation of cyber troops is gaining momentum. It has been established that incidents in the field of cybersecurity affect the livelihoods of consumers of information and many other services, as well as cyberattacks aimed at various objects in the infrastructure of electronic communications systems or control of technological processes. To increase the effectiveness of the fight against cybercrime, developed countries have long begun the appropriate work necessary to create their cybersecurity strategy (Nussipova et al., 2023).

Given the problem's relevance, the examination and evaluation of the role of public administration in addressing hybrid threats in cyberspace takes on a crucial significance. Specific countries were carefully chosen to conduct a comparative analysis based on their advanced cybersecurity infrastructure. France and Japan were identified as the countries with the most developed cybersecurity measures. Qualitative indicators reflecting the status of public administration systems in these countries as of mid-2024 were collected. Additionally, a comprehensive examination of hybrid threats in cyberspace was conducted, identifying distinct types of hybrid threats and their intended targets.

Literature review

Among the available academic research, a model is proposed that addresses the problem of hybrid threats in four stages, namely: 1) analysis and identification of hybrid threats; 2) designation and selection of tools; 3) building up resilience and capacity; 4) assessment and evaluation (Filipec, 2021; Coldea, 2022). At the same time, a study of hybrid threats and counter-hybrid solutions was carried out by analysing the state of affairs in Croatia, North Macedonia, and Bosnia and Herzegovina. It was established that hybrid threats combine military and non-military threats. Such threats include disinformation, cyberattacks, economic pressure, the deployment of regular armed formations, and regular forces (Mikac et al., 2022).

The topic of safeguarding against hybrid threats in the realm of cyberspace was thoroughly examined. It was concluded that it is necessary to develop a novel conceptual framework for addressing hybrid threats, incorporating tactics of deceit. Security initiatives predominantly concentrate on proactive strategies designed to thwart malicious actors from breaching the network. These applications attempt to use robust perimeters and endpoint protection by recognising and blocking malicious activities to detect and stop attackers before they can infiltrate (Steingartner et al., 2021; Lysenko et al., 2024).

The European Union has defined hybrid threats as diplomatic, military, economic and technological measures to destabilise a political adversary. These threats are one of the emerging security challenges in Europe and could shape the continent's future. According to EU policy, the primary responsibility for countering them lies with the member states; that NATO's role in ensuring security in Europe positions it as a crucial ally in military and conventional deterrence against hybrid threats (Lonardo, 2021).

The study of the definition of hybrid threats and the legal framework used to counter such threats is noteworthy. Hybrid threats can cause serious damage to basic infrastructure, making them an extremely powerful weapon in both peace and wartime. Even so, such threats must be combated through the means of law, as well as through prevention, resilience and education (Sanz-Caballero, 2023).

The strategies Finland, Germany, and the Netherlands employed in addressing hybrid threats are examined, considering their strategic cultures. The analysis reveals variations among the countries in their approaches to combating hybrid threats, particularly regarding security infrastructure and the extent of actions implemented to dissuade potential adversaries. These differences are mainly rooted in historical, institutional and political processes (Wijnja, 2021).

Furthermore, involving civil society in addressing hybrid threats is explored. The proactive engagement of civil society remains crucial in the joint effort to strengthen societal resilience, including by "supporting information pluralism, investing in civic awareness through education, and supporting an independent press that responds quickly to any disinformation" (Kalniete & Pildegovičs, 2021).

The examination of the potential resilience implementation in addressing hybrid threats across infrastructure, digital, and social domains, utilising a comprehensive, interdisciplinary, and government-wide strategy, is thorough and extensive. It was determined that sustainability-based decision-making contributes to problem-solving by analysing different digital systems' nested interdependencies and social sustainability (Vaseashta, 2022).

It was ascertained that European Union member states make heightened efforts to establish a unified institutional framework to address global and regional challenges (including hybrid ones) without abandoning the advantages of the Euro-Atlantic integration process in this aspect. The place of countering hybrid threats in the global security complex is determined by the fact that this issue is not limited to preventing this type of possible danger (Mumford, 2020). Nevertheless, de facto hybrid threats' source states often exploit contemporary global challenges for their strategic objectives (Grybko, 2021).

Some scholars argue that hybrid warfare strategically leverages all facets of a state's power to assert dominance over another state (Iancu et al., 2020). Simultaneously, it exploits the most vulnerable areas to achieve desired outcomes (Bratko et al., 2021).

Hybrid threats are perceived as threatening the nation's financial infrastructure. It was established that a sustained and all-encompassing effort to combat hybrid threats in this realm is imperative, relying on global collaboration. Simultaneously, the education of individuals across all age groups holds considerable significance. Such education should be aimed at developing critical thinking and resilience to the disinformation that currently surrounds us (Korauš et al., 2024).

In light of the above, the role of public administration in countering hybrid threats in cyberspace remains insufficiently studied. Public administration's proficient establishment and efficient functioning mitigate the proliferation of hybrid threats and intrusions in the cyber realm. This underscores the necessity for a comprehensive examination.

Objectives

The purpose of the study is to conduct research and assess public administration's role in countering cyberspace hybrid threats. Hence, the study aims to achieve the following objectives:

1. Identify specific types of hybrid threats in cyberspace and their targets;
2. Identify the principal subjects of public administration that are entrusted with the responsibility of countering hybrid threats in Ukraine's cyberspace.
3. To identify the major features that characterise the entities entrusted with the responsibility of countering hybrid threats in cyberspace in Ukraine, France and Japan;
4. Determine the main goals that hybrid threats in cyberspace are aimed at and the characteristics of how to counter them.

Methods

The research procedure involves several stages, namely: (1) analysis of scientific research on the existence of hybrid threats in cyberspace and their counteraction; (2) recognising distinct categories of hybrid threats in the digital realm and their intended targets; (3) pinpointing the primary entities within public administration, entrusted with the task of countering hybrid threats in Ukrainian cyberspace; (4) conducting a comparative task analysis of the entities entrusted with the responsibility of countering hybrid threats in cyberspace in Ukraine, France and Japan as of mid-2024; and (5) defining the role of public administration in countering hybrid threats in cyberspace.

The analysis of scholarly literature identified France and Japan as the most advanced nations in the world regarding cybersecurity. This status as a leading countries reflects the presence of highly effective public administration systems. Entities ensure cybersecurity in cyberspace and counter cyber threats. Accordingly, the above countries were chosen for comparison with Ukraine. Qualitative data were taken as indicators demonstrating the development of public administration entities entrusted with the responsibility of countering hybrid threats in cyberspace.

Drawing upon the procedure and methodology of the study, a comparative analysis of the objectives of the public administration entities, which are entrusted with the responsibility of ensuring cybersecurity in Ukraine, France and Japan, was carried out. The aforementioned entities are operational as of mid-2024. The examination was conducted on the roles of the examined entities as organisational frameworks in combating hybrid threats in the digital realm. Throughout the execution of this study, various empirical methodologies were employed, with a notable focus on the analysis-synthesis method, which made it possible to compare public administration bodies that are entrusted with the responsibility of countering hybrid threats in cyberspace. Several empirical methods were used during the present study, particularly the visual-graphic method.

Results

Following the comprehensive analytical research, we acquired relevant qualitative metrics that illustrate the advancement of the public administration system in the nations under analysis. The objectives, the primary functional aspects of the organisation's operations, mirror the pressing issues that must be tackled to effectively combat hybrid threats (Figure 1).

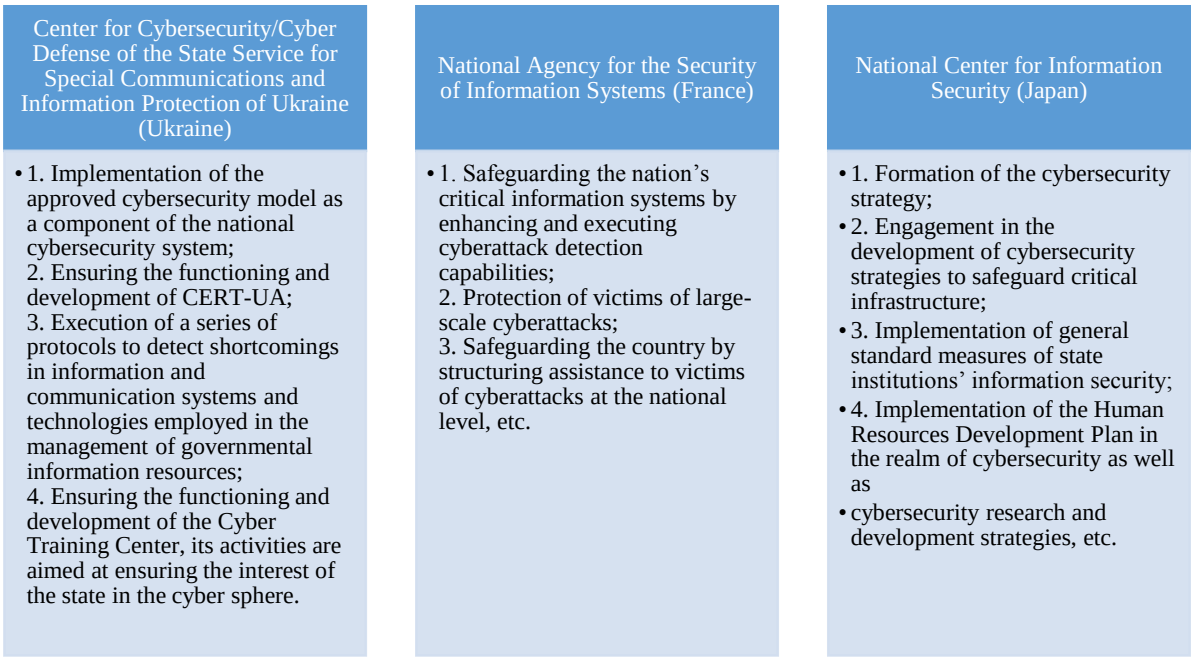

Figure 1. Objectives of public administration entities in the field of cybersecurity in Ukraine, France, Japan

The above results demonstrate that each country selected for analysis has one major subject: public administration in cybersecurity. Each of these entities is responsible for carrying out the authorised Cybersecurity Strategies and contributing to executing state policy in this field. In contrast, the cybersecurity agencies of France and Japan are assigned tasks of a more international scope, such as e.g. developing recommendations, implementing examinations and assessing threats and risks. In Ukraine, the tasks of the Cybersecurity/Cyber Defense Center of the State Service for Special Communications and Information Protection of Ukraine rather have a procedural nature.

It is essential to recognise the significant role that public administration plays in addressing hybrid threats in cyberspace. Figure 1 shows this role in the context of the objectives addressed by specific subjects of public administration in Ukraine, France and Japan. The prevalence of hybrid threats in the cyber domain is contingent upon adequate organisational support. Given the above, Ukraine may benefit from adopting the practices of France and Japan by establishing a dedicated entity to address hybrid threats in the digital domain. Currently, the Center for Cybersecurity/Cyber Defense is a structural unit of the State Service for Special Communications and Information Protection of Ukraine and not a separate

subject of public administration in this area. In this light, the separation of an individual subject could make it possible to carry out activities and coordinate tasks more comprehensively.

Based on the study findings, it was determined that Ukraine and France collaborate in cybersecurity through a formal Cooperation Agreement. The two nations work together to identify, prevent, and combat cyber aggression and espionage. Such actions are carried out by strengthening cyber resilience and protecting critical infrastructure from cyberattacks. That being said, the modernisation and reform of Ukraine's security architecture are supported, and international technical assistance is provided to Ukraine.

The analysis of the responsibilities of cybersecurity professionals and strategies for combating hybrid threats highlights the significance of incorporating contemporary technological advancements to address these challenges. The list of tasks of the studied entities should be constantly improved and predicted, taking into account possible hybrid threats in general and cyber threats in particular. It is imperative to consider global trends in cyber technology development, drawing from the expertise of advanced nations in the European Union and NATO. Furthermore, a critical factor in enhancing the importance and influence of the entities under study is the establishment of contemporary approaches to appropriate legal governance of their functions. Furthermore, it is crucial to employ a risk-focused strategy to enhance the capabilities of cybersecurity organisations and combat hybrid threats. Capacity enhancement must be conducted following a thorough analysis of the situation and the underlying factors that hinder an effective response to the entities under study in addressing hybrid threats in the cyber domain.

Establishing responsibilities for public administrative bodies in cybersecurity should be carried out with the mandatory consideration of international experience. Ukraine's integration into the European space provides an opportunity for cooperation with different countries in many areas. Such collaboration may be demonstrated through sharing accumulated expertise, innovative novel technologies to enhance cybersecurity and collaborative initiatives. It is essential to establish clear parameters for cooperation, particularly regarding refraining from involvement in the individual security matters of specific nations. The experience of cooperation between NATO and the EU in the direction of countering hybrid threats should be noted. The European Commission and the EEAS set up an interagency working group to counter hybrid threats, which are met at different levels. The above initiatives are designed to enhance mutual understanding among nations regarding the occurrences and mechanisms involved in combating hybrid threats in the digital realm and establish a

foundation for collaboration. Engaging in these events and endeavours will elevate the proficiency of cybersecurity stakeholders within each country, consequently bolstering the effectiveness of public administration in this field.

A comprehensive grasp of the challenges associated with mitigating hybrid threats in cybersecurity can significantly influence the strategies employed to combat these threats. Because of the above, each country should understand the types and nature of hybrid threats that can be applied to it. Failure to define the boundaries of an individual country in terms of countering hybrid threats will impact relations between countries and may become conflict-related.

Further, we examine hybrid threats through the lens of species differentiation. Using the comparative analysis technique, we delineate the prevalent types of hybrid threats in Ukraine, France and Japan from 2022 to 2024. Such hybrid threats as national, informational, and cybernetic threats were analysed.

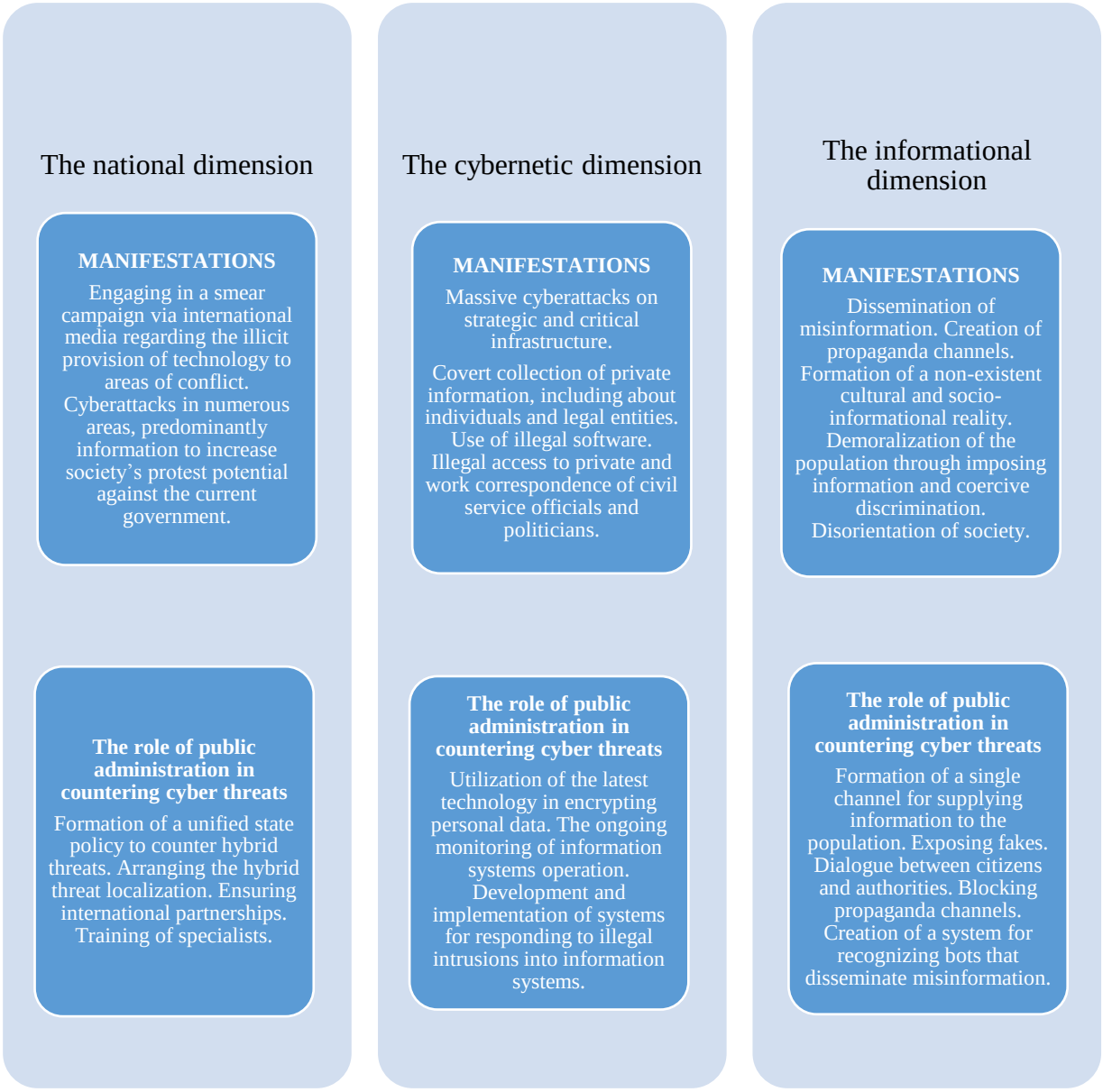

Figure 2. The prevalent dimensions of hybrid threats, their manifestations, and the efforts of public administration entities in combating them

Based on the information presented in Figure 2, it is feasible to derive conclusions about the targeted direction of hybrid threats in cyberspace. Such threats mostly relate to state authorities, national security, population awareness, and classified information. Delving into the manifestations of the above hybrid threats, it is important to acknowledge the numerous methods and tactics that are

continuously evolving. It should be noted that all the analysed types of hybrid threats significantly impact public administration entities' activities and the nationwide cybersecurity level. All threats are of strategic and critical importance and aim to acquire and further use illegally obtained information. Data is the target and focal point of illicit infringements. Furthermore, the scope of data is not confined solely to online resources. It encompasses data infrastructure and information and communication systems, serving as suitable conduits. With this in mind, the role and intervention of public administration should be comprehensive and extend to all possible future threats. Public administration entities can be involved in various areas to combat national, cyber, and information threats which are prevalent in society. Such areas are as follows:

- legal (development of normative acts);
- organisational (enhancement of the organisational structure);
- technical (optimisation of the information security system);
- psychological (cultivation of moral and ethical qualities in employees of public administration entities).

Utilising blockchain technology in public administration can also serve a pivotal function. Blockchain can furnish a dependable and lucid platform for data exchange between government bodies, law enforcement agencies, and the public in the context of hybrid threats. Its decentralised nature and data encryption can help counter cyberattacks and data manipulation, increasing the resilience of government systems. Given the above, one of the key applications of blockchain is to ensure information integrity and reliability, which is critical in combating disinformation and propaganda as components of hybrid threats. What is more, blockchain technology can effectively monitor supply chains and financial transactions, thereby enabling the detection and mitigation of economic pressures stemming from hybrid threats. However, it is important to acknowledge that integrating blockchain into public administration may present certain complexities.

First and foremost, it is the issue of scalability, as some blockchains may have limited bandwidth to process large amounts of data. Secondly, data privacy is also important, as blockchain is transparent, which can pose a problem for sensitive information. Thirdly, the legal regulation of the use of blockchain in the public sector has not yet been fully formed, which may create certain regulatory barriers. Moreover, concerns arise regarding the uniformity and compatibility of diverse blockchain platforms, posing challenges to their widespread integration. In essence, blockchain undoubtedly can enhance the resilience and effectiveness of public administration amidst hybrid threats. Nevertheless, a thorough analysis of

scalability, privacy concerns, regulatory compliance, and standardisation is imperative to effectively execute this plan.

The current article established that the significance of public administration in combating hybrid threats in cyberspace is evident through various actions tailored to the specific type of threat.

Discussion

The study findings reflect that the scholarly literature does not sufficiently address the role of public administration in countering hybrid threats in cyberspace. Furthermore, assessing the inherent capacities of each governmental organisation tasked with combating hybrid threats is imperative. The analysis should take place in the context of existing hybrid threats in cyberspace, the responsibilities available to the subject, and possible methods and counteraction means.

We share the opinion that contemporary challenges and intricate threats to peace and stability have sparked the development of novel strategies in the realm of cyber defence. It was collectively acknowledged that resolving security issues within the global information landscape, particularly in combating the latest hybrid information threats, can only be achieved through collaborative endeavours and adherence to international law (Avanesova et al., 2022).

Enhancing resilience through civil preparedness is a fundamental aspect of both NATO and EU strategies to counter hybrid threats, and cybersecurity, strategic communications, and military mobility are key areas the two organisations are working on (Jacuch, 2020). At the same time, the author does not fully address the role of state institutions in countering hybrid threats.

While sharing Coldea's (2022) opinion, it should be pointed out that there is no unanimously agreed definition of hybrid threats, war, or conflict. All major geopolitical actors use these terms, and two meanings generally stand out. First and foremost, it is a set of methods used in different ways and according to state or non-state actors' context to achieve specific results. The second meaning of hybrid threats can refer to an entity, a state, or a non-governmental organisation with the means and motives for influencing the opponent (Coldea, 2022).

The viewpoint of certain scholars as regards the interpretation of a critical axiom in the context of combating hybrid threats is contentious. In particular, "the hostile actor who uses this method tries to avoid the traditional response, disrupts their ability to respond effectively, and seeks to achieve their goals while remaining unattributed and unpunished" (Goudinov, 2023).

It is expedient to endorse the study's findings regarding the essential steps to enhance its resilience against disinformation as a hybrid threat and interference

in democratic processes. Such measures are as follows: 1) expanding the state's powers aimed at countering disinformation (Belkin et al., 2022); 2) broadening the inquiry into foreign intervention in information dissemination within the state; 3) defining public administration entities as global trendsetters in the information sphere; 4) involving civil society in countering disinformation (Kalniete & Pildegovičs, 2021).

Currently, we consider the position of scientists to be relevant to the end that strengthening security information in cyberspace in the face of hybrid threats is possible by following certain rules and actions. In particular, it is the renewal of digital transformations, increasing the level of society's digital literacy, and determining an equitable punishment level for engaging in cybercrime (Khriapynskyi et al., 2023).

Other academics have put forth a slightly different perspective on bolstering cybersecurity and combatting hybrid threats in the digital sphere. Specifically, they argue for the necessity of collaborative efforts across various sectors to proactively address, react to, and rebound from cyber offences. This includes involvement from governmental bodies, private enterprises, and non-governmental organisations. Given the current socio-political and information challenges, designing an effective cyber defence system is becoming increasingly imperative. Such a system will contribute to forming an effective mechanism for countering hybrid threats in the cyber sphere. Accordingly, there will be a proactive approach to addressing the dynamic shifts occurring in cyberspace and developing and implementing tools for a possible response to hybrid threats (Trofymenko et al., 2019). However, the researchers' perspectives appear rather broad and require further clarification.

It is expedient to draw attention to the viewpoint that hybrid threats are hostile actions that involve the simultaneous use of two or more threats (Jayantho et al., 2020). Simultaneously, they are under the control or coordination of a distinct entity, whether a state or non-state entity. It is worth mentioning that hybrid threats currently represent the predominant type of threat within the European security framework (Ozoliņa & Struberga, 2023).

The stance regarding the necessity of NATO's adjustment to non-conventional threats to uphold stability and security in an evolving security landscape appears justified. The author underscores the need for NATO allies to prioritise the development of strategies and action plans aimed at tackling new challenges. Such challenges include new technologies, energy security, climate change, hybrid threats and cyber threats (Halili, 2023).

Aligned with Sarjito's (2024) perspective, it is crucial to recognise the significance of intelligence in maintaining situational awareness, shaping political

strategies, and managing risks in hybrid warfare contexts. The author emphasises the need for leaders and organisations to adapt to work together and address hybrid warfare's challenges (Sarjito, 2024).

Further examination is necessary to assess each governmental body's true capacities for addressing hybrid threats. The analysis should take place in the context of existing hybrid threats in cyberspace, the responsibilities available to the entity, and possible methods and means of counteraction. Examination of international public administration experience in these matters will also be necessary.

Conclusions

The complexity and adaptability of these connections were effectively showcased through a comprehensive examination of public administration's role in addressing hybrid threats in cyberspace. The present study identified the public administration's role in addressing hybrid cyber threats in Ukraine, France and Japan. A comprehensive analysis was conducted to examine the responsibilities assigned to these entities, highlighting both shared characteristics and potential best practices that can be adopted.

An analysis of the prevalent types of hybrid threats, such as national, informational, cybernetic was carried out, specific actions of public administration entities to counter these threats were identified. It was determined that hybrid threats mostly relate to state's authority, national security, population awareness, classified information. Still, when identifying the manifestations of the above hybrid threats, it is indispensable to recognise that many evolving methods and tactics are at play.

Thus, the study addressed the role of public administration in countering hybrid threats in cyberspace, and its importance was confirmed. The prevalence of hybrid threats targeting the cyber domain is contingent upon adequate organisational support. It is evident that the cybersecurity agencies of France and Japan are tasked with global responsibilities and duties. For example, elaborating recommendations, implementing examinations, assessing threats and risks. In Ukraine, the tasks and responsibilities of the Cybersecurity/Cyber Defense Center of the State Service for Special Communications and Information Protection of Ukraine are primarily procedural.

At the same time, Ukraine can leverage the expertise of France and Japan by establishing a specialised body dedicated to combating hybrid threats in the digital domain. This distinct entity will enhance the efficiency of operations and facilitate more cohesive task coordination.

Recommendations

The prospects of further research are as follows:

- analysis of the actual capabilities of each public administration entity being endowed with the duty to counteract hybrid threats;

- comprehensive analysis of existing hybrid threats in cyberspace and the entity's responsibilities and possible methods and ways of countering such threats;

- international experience of public administration in countering hybrid threats in cyberspace;

- exploration of the potential establishment of a distinct entity in Ukraine dedicated to mitigating hybrid threats in the realm of cyberspace.

References

Avanesova, N., Serhiienko, Y., & Lyubushin, R. (2022). Strengthening the state cyber defense and creating of cyber troops: State, problems and organisational-economic measures for Ukraine. *Economic Innovations*, *24*(1(82)), 25-40. https://doi.org/10.31520/ei.2022.24.1(82).25-40

Belkin, L., Iurynets, Ju., Sopilko, I., & Belkin, M. (2022). Culture and the use of information understanding in the field of national security (a case study of Ukraine). *Journal of International Legal Communication, 5*(2), 36-58. https://doi.org/10.32612/uw.27201643.2022.5.pp.36-58

Bradshaw, S., & Howard, P. N. (2019). The global disinformation order. 2019 Global Inventory of Organised Social Media Manipullation. Oxford: Oxford Institute Study. Retrieved from https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

Bratko, A., Zaharchuk D., & Zolka, V. (2021). Hybrid warfare – a threat to the national security of the state. *Revista de Estudios en Seguridad Internacional, 7*(1), 147-160. https://doi.org/10.18847/1.13.10

Coldea, F. (2022). Intelligence Challenges in Countering Hybrid Threats. *National Security and the Future, 23*(1). https://doi.org/10.37458/nstf.23.1.2

Filipec, O. (2021). Preventing hybrid threats: From identification to an effective response. *European Studies, 8*(1), 17-38. https://doi.org/10.2478/eustu-2022-0063

Goudinov, I. (2023). Application of innovative systems for achieving compliance in countering hybrid threats. *Bulgarian Journal of International Economics and Politics, 3*(1), 69-90. https://doi.org/10.37075/BJIEP.2023.1.05

Grybko, O. (2021). Countering hybrid threats in the context of changing global environment. *Public Administration and State Security Aspects,* 1(1), 66-74. https://doi.org/10.52363/passa-2021.1-7

Halili, A. (2023). Non-traditional security threats and NATO's Response in the contemporary security environment. *SEEU Review*, *18*(2), 148-162. https://doi.org/10.2478/seeur-2023-0095

Iancu, N., Fortuna, A., & Barna, C. (2020). Countering hybrid threats: lessons learned from Ukraine. *NATO*. Retrieved from https://www.nato.int/cps/en/natohq/topics_142012.htm?

Jacuch, A. (2020). Countering hybrid threats: resilience in the EU and NATO's strategies. *The Copernicus Journal of Political Studies*, *1*, 5-26. https://doi.org/10.12775/CJPS.2020.001

Jayantho, S., Runturambi, A. J. S., Ras, A. R., & Widiawan, B. (2020). Pemodelan Sistem Dinamis Stratejik Intelijen Dalam Meminimalisasi Ancaman Spionase dan Pencurian Privasi Big Data Di Era Industri 4.0. *Jurnal Kajian Stratejik Ketahanan Nasiona*, *3*(2). Retrieved from https://scholarhub.ui.ac.id/jkskn/vol3/iss2/6

Kalniete, S., & Pildegovičs, T. (2021). Strengthening the EU's resilience to hybrid threats. *European View*, *20*(1), 23-33. https://doi.org/10.1177/17816858211004648

Khriapynskyi, A., Khmyrov, I., Svoboda, I., Shevchuk, M., & Iastrebova, V. (2023). State information security strategies in conditions of hybrid threats. *Amazonia Investiga*, *12*(69), 84-93. https://doi.org/10.34069/AI/2023.69.09.7

Korauš, A., Jančíková, E., Gombár, M., Kurilovská, L., & Černák, F. (2024). Ensuring financial system sustainability: Combating hybrid threats through anti-money laundering and counter-terrorist financing measures. *Journal of Risk and Financial Management*, *17*(2), 55. https://doi.org/10.3390/jrfm17020055

Lonardo, L. (2021). EU law against hybrid threats: A first assessment. *European Papers*, *6*(2), 1075-1096. https://doi.org/10.15166/2499-8249/514

Lysenko, S., Bobro, N., Korsunova, K., Vasylchyshyn, O., & Tatarchenko, Y. (2024). The role of artificial intelligence in cybersecurity: Automation of protection and detection of threats. *Economic Affairs*, 69(1Special), 43-51. https://doi.org/10.46852/0424-2513.1.2024.6

Mikac, R., Mitrevska, M., & Smajić, M. (2022). Hybrid threats and counter-hybrid solutions: A Comparative case study analysis of Croatia, North Macedonia, and Bosnia and Herzegovina. *Politics in Central Europe*, *18*(3), 375-395. https://doi.org/10.2478/pce-2022-0017

Mumford, A. (2020). Ambiguity in Hybrid Warfare. *Hybrid CoE*. Retrieved from https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-24-ambiguity-in-hybrid-warfare/

NATO. (2021). What is NATO doing to address hybrid threats? Retrieved from https://www.nato.int/cps/en/natohq/news_183004.htm

Nussipova, A., Khussainova G., Kabilova R., & Aliyarov, E. (2023). Estrategia De Comunicaciones De Seguridad De La información Como Requisito Previo Para Contrarrestar La Guerra híbrida: Experiencia Mundial». *Revista Latina De Comunicación Social*, *82*. https://doi.org/10.4185/rlcs-2024-2134

Ozoliņa, Z., & Struberga, S. (2023).Subjective perception of hybrid threats in Latvia. *Lithuanian Annual Strategic Review*, *20*(1), 119-152. https://doi.org/10.47459/lasr.2023.20.6

Sanz-Caballero, S. (2023). The concepts and laws applicable to hybrid threats, with a special focus on Europe. *Humanities and Social Sciences Communications*, *10*, 360(2023). https://doi.org/10.1057/s41599-023-01864-y

Sarjito, A. (2024). The role of intelligence through the formulation of national defense policy in hybrid war. *Pandita: Interdisciplinary Journal of Public Affairs*, *7*(1), 74-88. https://doi.org/10.61332/ijpa.v7i1.152

Steingartner, W., Galinec, D., & Kozina, A. (2021). Threat defense: Cyber deception approach and education for resilience in hybrid threats model. *Symmetry*, *13*(4), 597. https://doi.org/10.3390/sym13040597

Trofymenko, O., Prokop, Y., Loginova, N., & Zadereyko O. (2019). Cybersecurity of Ukraine: Analysis of the current situation. *Ukrainian Information Security Research Journal*, *21*(3).

Vaseashta, A. (2019). Applying resilience to hybrid threats in infrastructure, digital, and social domains using multisectoral, multidisciplinary, and whole-of-government approach. *Building Cyber Resilience against Hybrid Threats*. Amsterdam: IOS Press. https://doi.org/10.3233/NICSP220017

Wijnja, K. (2021). Countering hybrid threats: Does strategic culture matter? *Defence Studies*, *22*(1), 1-19. https://doi.org/10.1080/14702436.2021.1945452