UDC 342.951:327.39
DOI: 10.32518/sals1.2025.165

Соціально-правові студії. 2025. Т. 8, № 1
Social & Legal Studios. 2025. Vol. 8, No. 1

State information policy in the context of hybrid threats: Legal and political aspects

Sergii Balan*

PhD in Political Sciences, Senior Researcher
V.M. Koretsky Institute of State and Law of National Academy of Sciences of Ukraine
01601, 4 Tryokhsvyatytelska Str., Kyiv, Ukraine
https://orcid.org/0000-0002-9421-7037

Liudmyla Balan

Independent Researcher
Dive and Discovery Research Ltd.
02000, 8 Kostelna Str., Kyiv, Ukraine
https://orcid.org/0009-0008-5819-3323

Vadym Vorotynskyy

Doctoral Student
V.M. Koretsky Institute of State and Law of National Academy of Sciences of Ukraine
01601, 4 Tryokhsvyatytelska Str., Kyiv, Ukraine
https://orcid.org/0009-0008-2858-9298

Iryna Rybak

PhD in Political Sciences, Associate Professor
"KROK" University
03113, 30-32 Tabirna Str., Kyiv, Ukraine
https://orcid.org/0000-0002-4165-8154

Volodymyr Tarasiuk

Doctoral Student
V.M. Koretsky Institute of State and Law of National Academy of Sciences of Ukraine
01601, 4 Tryokhsvyatytelska Str., Kyiv, Ukraine
https://orcid.org/0000-0003-1863-3028

Abstract. The study aimed to identify the main ways to optimise the state information policy in order to strengthen the ability to withstand complex hybrid challenges. The study examined modern approaches to the definition of hybrid threats and their impact on the information sphere of the state. The legal mechanisms of information policy regulation in the context of countering hybrid threats have been considered, and the effectiveness of political tools for formulating and implementing the state's information strategy in the context of hybrid warfare is assessed. The analysis showed the complex and multidimensional nature of hybrid threats, which significantly complicates the process of forming an effective information policy. In the period from 2014 to 2024, Ukraine's legal and regulatory framework in the field of information security has developed significantly but still has gaps, in particular in the flexibility of legal norms and mechanisms of interagency coordination. The assessment of the effectiveness of policy instruments showed significant progress in strengthening Ukraine's institutional capacity to counter information threats but revealed the need for further improvement of coordination mechanisms and development of public-private partnerships. The study proposed a conceptual model of an integrated system of state information policy that demonstrates high efficiency in responding to various hybrid threat scenarios. The key success factor is the system's ability to constantly adapt and learn. The results emphasised the need for an integrated approach to information security, including legal, institutional, technological, and

Suggested Citation **Article's History**: Received: 02.11.2024 Revised: 05.03.2025 Accepted: 26.03.2025

Balan, S., Balan, L., Vorotynskyy, V., Rybak, I., & Tarasiuk, V. (2024). State information policy in the context of hybrid threats: Legal and political aspects. *Social & Legal Studios*, 8(1), 165-178. doi: 10.32518/sals1.2025.165.

*Corresponding author

social aspects. Special attention was paid to the development of research capacity in the field of information security and the introduction of innovative technologies to counter emerging hybrid threats. The results of the study have expanded the theoretical understanding of information policy in the context of hybrid threats, which has allowed to provide practical recommendations for improving the relevant state strategies

Keywords: national security; cybersecurity; disinformation; strategic communications; media literacy; cyber defence

Introduction

In today's world, where information technologies are rapidly evolving, and the geopolitical landscape is increasingly complex, the state information policy has become critically important. Hybrid threats, which combine elements of conventional and unconventional warfare, pose new challenges to national security and sovereignty. These threats often materialise in the information domain, highlighting the necessity of an effective information policy to protect and advance national interests. The growing role of information as a strategic resource and an instrument of influence in international relations drives the urgency of this study. It seeks to address gaps in understanding the relationship between legal norms, political decisions and practical measures in information security. Furthermore, analysing Estonia's, the United States, and the EU's experiences in countering hybrid threats can provide valuable insights into improving national information policy strategies.

This research responds to the need for a comprehensive analysis of the legal and political dimensions of state information policy formation and implementation in hybrid threat contexts. Existing regulatory approaches often fail to effectively address modern challenges such as disinformation, cyberattacks, and public opinion manipulation. This highlights the urgent need to develop new strategies and mechanisms tailored to hybrid threats while ensuring a balance between information freedom and national security. An analysis of the scientific literature demonstrates the growing interest of researchers in this area. However, a comprehensive understanding of the relationship between legal norms, political decisions and practical measures in the field of information security remains insufficiently developed

Regarding the legal aspects of information policy and hybrid threats, A. Sari's (2020) study introduced "legal resilience" as a key element in countering such threats. The author emphasised the need to adapt legal systems to new challenges, but the issue of practical implementation of this concept in national legislation remains open. Developing this topic, E. Reichborn-Kjennerud and P. Cullen (2022) conducted a thorough analysis of the concept of "hybrid warfare", emphasising its multidimensionality, including information, cyber and economic aspects. However, their work does not fully reveal the specifics of the formation of the state's information policy in such conditions. Complementing this analysis, H. Ördén (2020) examined the EU's policy on information threats, pointing to the tendency to "defer the essence" in the EU's approaches, which can lead to an ineffective response to hybrid threats and, as evidenced by Ukraine's current situation, has led to a catastrophic lack of a proper political, legal, institutional and social mechanism for responding to information operations discrediting the Ukrainian state.

When analysing the international landscape, M. Mälksoo's (2020) work on the EU and NATO's approaches to countering hybrid threats through ontological security management is particularly noteworthy. This approach offers new insights into the strategic aspects of information policy but requires further development to account for national contexts. In the same vein, M.L. Miller and C. Vaccari (2020) analysed digital threats to democracy, offering a comparative analysis and possible solutions. Their study highlighted the need for a balance between ensuring freedom of information and countering disinformation, which is a key challenge for modern information policies. Adding to this discussion, D. Ghelani (2022) examined aspects of cybersecurity, emphasising the need for a comprehensive approach to cyber threats that includes technical, political, and legal aspects.

At the same time, C. Whyte (2020) considered the problem of disinformation created by artificial intelligence as a multilevel challenge for public policy. This work highlighted the need to develop new approaches to regulating the information space in the context of technological innovation. Amid current geopolitical challenges, A. Khorram-Manesh *et al.* (2023) analysed the social and health impacts of Ukraine's hybrid war, highlighting the need to consider the broad consequences of hybrid threats in information policy. Expanding the theoretical framework, D. Schiller (2024) proposed new approaches to understanding information in the modern world, which can serve as a basis for rethinking the principles of the state's information policy in the context of hybrid threats. To conclude the review of the scientific discourse on this issue, it is worth mentioning the study by T. Voropayeva and N. Averianova (2021), which focused on the priority areas of Ukraine's state policy in the field of information and economic security. The authors emphasise the importance of the "smart power" strategy in countering hybrid threats, but the specific mechanisms for implementing this strategy need further study.

In summary, despite extensive research, several aspects of state information policy in the context of hybrid threats remain underexplored. Key issues requiring further analysis include adapting legislation to emerging information threats, improving coordination among state institutions, and developing strategies to engage civil society in countering hybrid threats. In addition, an important area for further research is the development of methodological approaches to assessing the effectiveness of information policy in hybrid conflicts. Therefore, this study aimed to identify key areas for enhancing state information policy on hybrid threats, with a focus on legal and political aspects. To achieve this goal, the study was focused on:

1) analyse contemporary approaches to defining hybrid threats and their impact on the state's information sphere.

2) examine legal mechanisms for regulating information policy in the context of hybrid threat mitigation.

3) assess the effectiveness of political instruments in shaping and implementing the state's information strategy amid hybrid warfare.

Materials and methods

The study's source base comprises Ukrainian legal acts on information security, including, Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring Cybersecurity of Ukraine" (2017), Decree of the President of Ukraine No. 47/2017 "On the Decision of the National Security and Defence Council of Ukraine of 29 December 2016 "On the Doctrine of Information Security of Ukraine" (2016), and also Law of Ukraine No. 2404-VI "On Public-Private Partnership" (2010). The analysis included international documents such as the Joint Communication to the European Parliament and the Council: "Joint Framework on Countering Hybrid Threats – A European Union Response" (2016), as well as U.S. legislation, including Public Law of United States No. 115-278 "Cybersecurity and Infrastructure Security Agency Act" (2018) and Executive Order of the President of United States No. 14028 "Improving the Nation's Cybersecurity" (2021). Additionally, Estonia's cybersecurity regulations (Ministry of Economic Affairs and Communications of the Republic of Estonia, 2019) were examined.

Key sources of information included reports and analyses from international organisations, notably the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE, 2021). Cyber threat statistics from the KnowBe4 report (Cyberattacks on infrastructure…, 2024) were examined, and the National Cyber Security Index (2024) was utilised to evaluate Ukraine's cybersecurity progress. To achieve this goal, the research methodology integrated qualitative and quantitative approaches to analyse Ukraine's legal framework, international regulatory documents, and policy implementation mechanisms. Content analysis was employed to systematically examine legal acts, strategic documents, and scholarly publications on information security, enabling the identification of key trends in hybrid threat development. The institutional approach was applied to examine legal mechanisms regulating information policy and the functions of specialised bodies, facilitating an assessment of the institutional structure's effectiveness. Scenario modelling was employed to analyse potential hybrid threat scenarios, enabling an assessment of the proposed information policy model's adaptability. A SWOT analysis was conducted to evaluate the strengths, weaknesses, opportunities, and threats in Ukraine's information policy, facilitating the systematisation of findings and the formulation of informed recommendations for enhancing information policy amid hybrid threats. The authors examined the evolution of the "hybrid threats" concept and its impact on the state's information sphere.

The study assessed the effectiveness of political instruments in shaping and implementing the state's information strategy amid hybrid warfare. It examined the institutional framework supporting Ukraine's information policy, particularly the roles of specialised bodies such as the National Coordination Centre for Cybersecurity and the Centre for Strategic Communications and Information Security. Additionally, it evaluated interagency coordination mechanisms and public-private partnerships in information security. A conceptual model for an integrated state information policy system is developed. Based on this model, the system's response to various hybrid threat scenarios was simulated, enabling an assessment of its adaptability and effectiveness in addressing information security challenges. The study employed expert assessments to evaluate the effectiveness of government programs and strategies in information security. Specifically, it analysed the implementation of Ukraine's Cybersecurity Strategy 2016-2020, as reflected in the draft Cybersecurity Strategy of Ukraine 2021-2025 (2021).

To assess Ukraine's progress in information security from 2014 to 2024, key performance indicators are examined using data from international rankings, including the National Cyber Security Index (2024), along with statistics on cyber incidents and information attacks. The study also explored the impact of hybrid threats on democratic processes and institutions, focusing on mechanisms of electoral interference and public opinion manipulation through information operations. Additionally, it examined international approaches to countering hybrid threats, analysing the information policies of the EU, NATO, and countries such as the United States, Estonia, and the United Kingdom – selected for their extensive experience in addressing hybrid threats and developing comprehensive information security strategies. Particular attention was given to international cooperation mechanisms in cybersecurity and threat intelligence sharing.

Results

Analysis of contemporary approaches to defining hybrid threats and their impact on the information sphere of the state. Between 2014 and 2024, the concept of hybrid threats gained prominence in scientific and political discourse due to the increasing complexity and multidimensional nature of modern conflicts, which extend beyond traditional military confrontation. M. Galeotti (2018) defines hybrid threats as the strategic use of various state influence mechanisms, including diplomatic, informational, military, and economic instruments, to achieve objectives without formally declaring war. This interpretation highlights the multifaceted nature of modern challenges, which often emerge in the ambiguous space between peace and open conflict. Ukrainian researchers, particularly Kh.O. Mishchenko (2020), expand this concept by emphasising the information dimension, defining hybrid threats as a combination of influence mechanisms designed to undermine statehood, including information manipulation, economic pressure, cyberattacks, and the use of proxy forces. Notably, the concept of hybrid threats is dynamic, evolving alongside technological advancements and geopolitical shifts. For instance, a study by the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE, 2021) highlights the increasing role of artificial intelligence and quantum computing in shaping new forms of hybrid threats.

Analysing current definitions of hybrid threats reveals several key types, particularly relevant to the information sphere, that collectively pose complex challenges to national security. The most prevalent type is disinformation campaigns, which systematically spread false or manipulative information to shape public opinion and influence decision-making. L. Rosenberger (2020) highlights how these campaigns undermine democratic processes and national security. Equally significant are cyberattacks, which target information systems to disrupt operations, steal data, or inflict economic damage. The severity of this issue is highlighted by statistics, with cyberattacks increasing by 600% during the COVID-19 pandemic. Closely related are social media influence operations, which exploit digital platforms to manipulate public opinion, polarise society, and erode trust in government institutions (Zelenov, 2024).

Research from the Oxford Internet Institute indicates that over 80 countries have established systems for leveraging social media to shape public discourse (Bradshaw *et al.,* 2021). The fourth type is economic influence through information tools, which leverages various sources and channels to destabilise the economy, manipulate market mechanisms, or undermine financial stability. The fifth type, known as lawfare (legal warfare), involves the strategic exploitation of legal frameworks and international law to achieve geopolitical objectives. O.F. Kittrie (2022) examines how certain states manipulate international legal instruments to legitimise aggressive actions in the information space. For instance, the Russian Federation frequently cites the principles of responsibility to protect (R2P) and self-defence to justify its cyber operations against other states. In the 2008 conflict with Georgia, Russia justified it cyberattacks on Georgian government websites and infrastructure as a "defence" of the Russian-speaking population in South Ossetia, manipulating international legal principles to legitimise its actions in cyberspace.

These information threats are highly adaptable, difficult to detect and attribute, and capable of rapid escalation. Their synergistic nature amplifies their impact, creating a complex and dynamic challenge for state information security. In the current geopolitical landscape, hybrid threats pose an increasingly complex and multifaceted challenge to national information security, impacting various aspects of public life, including politics, economics, and culture. These threats undermine state authority, eroding public trust in government institutions, the media, and other key entities (Van Raemdonck & Meyer, 2024). This process is closely linked to societal polarisation, driven by targeted manipulative information campaigns. As P.M. Krafft and J. Donovan (2020) demonstrate, such campaigns not only deepen existing social, ethnic, and political divisions but also foster radicalisation and the spread of extremist ideologies. The economic impact of hybrid threats is particularly significant, especially for developing countries. A notable example is the 2022 cyberattack on Costa Rica's government agencies, which resulted in unprecedented economic losses amounting to 2.4% of the country's annual GDP (Vergara Cobos, 2024).

This incident underscores the vulnerability of national economies to digital threats and the urgent need for robust cyberdefense systems. Equally concerning is the impact of hybrid attacks on critical infrastructure. A recent KnowBe4 analysis highlights a significant rise in both the frequency and scale of such cyberattacks. Between 2023 and 2024, over 420 million cyberattacks were recorded, averaging 13 incidents per second – a 30% increase from the previous year. The U.S. energy sector proved particularly vulnerable, with approximately 60 new power grid vulnerabilities identified daily (Cyberattacks on infrastructure…, 2024). These findings highlight the urgent need for more effective strategies to safeguard critical infrastructure. Hybrid threats significantly affect democratic processes, particularly through electoral manipulation and political interference (Davies, 2021). These actions undermine the legitimacy of democratic institutions and contribute to broader political destabilisation. Hybrid threats significantly affect democratic processes, particularly through electoral manipulation and political interference (Davies, 2021). These actions undermine the legitimacy of democratic institutions and contribute to broader political destabilisation. These operations target national identity, undermine cultural values, and create artificial conflicts based on cultural differences. The Ukrainian case exemplifies the destructive impact of identity crisis technologies and so-called "identity-destructive traditional weapons" (Kresina, 2024).

The cumulative impact of hybrid threats on national information security must be emphasised. While individual incidents may appear inconsequential, their convergence creates a complex web of threats. This underscores the need for states to develop comprehensive, multi-level countermeasures that address the interconnections between various components of information security and safeguard national interests in the information space. To address these challenges, countries are adopting comprehensive cyber defence and information resilience programs. Specifically, Ukraine's Cybersecurity Strategy, approved by Decree of the President of Ukraine No. 447/2021 (2021), aims to enhance the national cyber defence system, bolster the defence sector's ability to combat cyber threats, and ensure the security of the digital space. At the global level, cooperation mechanisms to combat hybrid threats are being developed. For instance, NATO's specialised Centre of Excellence coordinates member states' efforts in this area (Hybrid CoE, 2021).

In conclusion, the analysis of contemporary approaches to hybrid threats and their impact on the state's information sphere highlights the complexity of this phenomenon. The study identified various hybrid threats, including disinformation campaigns, cyberattacks, social media influence operations, and the abuse of legal mechanisms. Emphasis was placed on the adaptability of these threats and their potential for rapid escalation. The analysis of hybrid threats' impact on state information security underscores the need for a comprehensive counterstrategy. Additionally, the evolving nature of these threats necessitates continuous updates to their definition and assessment, offering opportunities for further research.

Study of legal mechanisms for regulating information policy in the context of countering hybrid threats. As hybrid threats become increasingly complex and intense, legal mechanisms for regulating information policy are essential to national security. This section provides a detailed analysis of Ukraine's legal framework, international practices, and prospects for legislative improvements in countering information threats. Ukraine's legal framework for information policy and security has undergone significant revisions, particularly between 2014 and 2024. A key document shaping state policy in this area is Decree of the President of Ukraine No. 47/2017 "On the Decision of the National Security and Defence Council of Ukraine of 29 December 2016 "On the Doctrine of Information Security of Ukraine" (2016). This regulatory act defines the state's strategic interests in information security, identifies potential risks, and establishes the main priorities and directions of government strategy in information policy.

A significant advancement in Ukraine's legislative framework was the adoption of Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring Cybersecurity of Ukraine" (2017). This law establishes the foundation for safeguarding the critical interests of individuals, civil society, and the state in the digital domain. It defines key objectives, strategic priorities, and fundamental principles of state cyber defence policy. Additionally, it delineates the

responsibilities of government institutions, private enterprises, NGOs, and individuals while introducing mechanisms for coordinating efforts to ensure the robust protection of national cyberspace. Decree of the President of Ukraine No. 447/2021 (2021) establishes a hierarchy of Ukraine's key interests in cyberspace protection. It identifies existing and potential digital threats that could undermine citizens' fundamental rights, societal stability, and national security. The strategy also outlines priority directions and a conceptual framework for developing and implementing state policy to ensure a secure digital environment, benefiting individuals, civil society, and the state as a whole. Despite significant progress in legislative development, certain gaps and shortcomings remain. Notably, clearer mechanisms for coordinating state agencies in countering information threats are needed. The current interagency cooperation framework often lacks the agility to respond effectively to the rapidly evolving information environment, potentially weakening efforts to combat hybrid threats.

An analysis of global legal approaches to regulating the information space amid hybrid threats reveals diverse methods and strategies employed by states and supranational entities. The European Union has developed a comprehensive strategy to combat hybrid threats, integrating both regulatory and structural initiatives. The EU adopted the Joint Communication to the European Parliament and the Council "Joint Framework on Countering Hybrid Threats a European Union Response" (2016), which outlines key strategic directions in this domain. In 2017, the European Centre of Excellence for Countering Hybrid Threats was established to foster strategic discussions and conduct analytical research on hybrid challenges. The United States also prioritises legislative regulation of information security. Public Law of United States No. 115-278 (2018) created a specialised agency to protect critical infrastructure from cyber threats. Executive Order of the President of United States No. 14028 (2021) introduced enhanced security standards for government agencies and their contractors. Estonia, recognised as a leader in cyber defence, offers a particularly noteworthy approach. Its Cybersecurity Strategy 2019-2022 prioritises strengthening cyber resilience and enhancing international cooperation (Ministry of Economic Affairs and Communications of the Republic of Estonia, 2019). The Estonian model follows a total defence concept, integrating state institutions, the business sector, and civil society organisations into cybersecurity efforts.

An analysis of Ukrainian legislation and international practices reveals significant gaps in the regulatory framework for countering information threats. These deficiencies hinder efforts to maintain effective information security amid rapid technological advancements and evolving hybrid challenges. The absence of a clear legal framework defining the criminal nature of Russian hybrid influence, particularly in the context of prolonged latent aggression against Ukraine, remains a significant challenge. Cyberterrorism has become a key instrument in the aggressor's warfare, especially following the large-scale invasion on February 24, 2022. However, both national and international legal systems continue to treat such acts of information terrorism as secondary concerns.

First, the rigidity of legal norms remains a critical issue, stemming from the rapid evolution of information technology and the ever-changing nature of threats. The existing legal framework often fails to keep pace with reality, creating gaps that criminals can exploit. Addressing this challenge requires the development of more adaptive legislative instruments capable of responding swiftly to shifts in the information landscape. The second major challenge is the inefficiency of coordination among key stakeholders in information security. This issue extends beyond intergovernmental communication to include collaboration between the government, the private sector, and non-governmental organisations. Weak coordination results in functional redundancies, inefficient resource allocation, and a diminished overall capacity to counter information threats effectively. Addressing this challenge requires a comprehensive approach to establishing a unified management system and enhancing coordination in information security. Particular attention must be given to balancing national security with the protection of civil rights and freedoms, a complex task at the core of effective information policy formulation.

Enhancing security in the information space often entails certain restrictions, raising concerns about potential violations of fundamental rights, including privacy and free expression. Striking an optimal balance between security and civil liberties is crucial for developing and modernising information security legislation. Given the global nature of modern information threats, strengthening international cooperation is also essential for improving legal regulation. Effective mechanisms for international data exchange and coordinated responses to cyber threats are urgently needed. This requires not only aligning national legislation with international standards but also strengthening Ukraine's role in shaping the global information security framework. Additionally, fostering public-private partnerships is essential for advancing cybersecurity legislation. Given the substantial private ownership of strategically important infrastructure, effective collaboration between the state and business is vital for ensuring the country's information security. This necessitates the development of legislative measures to encourage businesses' active participation in cyberspace protection, alongside clear definitions of cooperation mechanisms between the public and private sectors in cyber defence.

Given the identified shortcomings, the modernisation of the legislative framework for addressing information challenges should focus on several strategic areas. A priority is the creation of a comprehensive regulatory act on countering hybrid threats, defining key principles, tools, and definitions. This document should serve as the foundation for an integrated system ensuring the country's information security. Simultaneously, attention should be given to optimising algorithms for rapid response to information challenges, including the creation of specialised units and the development of targeted cooperation schemes among information security actors. An important step is to strengthen cyber defence regulations for entities managing critical infrastructure, thereby enhancing the security of strategically important elements. An urgent task is aligning Ukraine's legal framework with international standards and best practices in cyberspace protection, facilitating the country's integration into the global system for countering information threats.

Assessment of the effectiveness of political instruments in shaping and implementing state information strategy amid hybrid warfare. Amid escalating global geopolitical tensions and increasing hybrid challenges, particularly between 2014 and 2024, evaluating the effectiveness of state mechanisms for shaping and implementing information

strategy is crucial. This section provides a comprehensive analysis of existing instruments, assesses their effectiveness, and proposes strategies for optimising political measures to counter hybrid threats in the information domain. Over the past decade, Ukraine's information strategy in hybrid confrontation has undergone significant transformation, shaped by interrelated political mechanisms. This evolution was driven by the need to address escalating information threats and establish an effective system for countering hybrid challenges. A cornerstone of this system is strategic planning, reflected in the adoption of the updated Cybersecurity Strategy of Ukraine in 2021 (Decree of the President of Ukraine No. 447/2021, 2021). This regulatory act defined the key directions of state policy in the information sector, focusing on securing the information environment, fostering its development within Ukraine, and safeguarding citizens' constitutional right to access information.

The adoption of this strategy addressed the urgent need for a comprehensive approach to information security and laid the groundwork for enhancing the implementation of state information policy. Alongside strategic planning, the institutional framework for information policy was reinforced. A key step was the establishment of the Ministry of Information Policy (Decree of the President of Ukraine No. 449/2014, 2014), later restructured as the Ministry of Culture and Information Policy in 2019 (Resolution of the Cabinet of Ministers of Ukraine No. 829, 2019). This transition aimed to centralise the management of the information domain, enhance coordination among agencies, and strengthen state efforts to counter information threats. Additionally, specialised units were established within the Security Service of Ukraine, the Ministry of Defence, and other state agencies, enhancing the state's information security capabilities and supporting the development of a multi-layered system for protecting national interests in the information sphere.

The legal and regulatory framework has been a crucial element in developing an effective information strategy. Key legislative measures, including Law of Ukraine No. 2163-VIII (2017) and Law of Ukraine No. 2469-VIII (2018), along with the modernisation of Law of Ukraine No. 2657-XII (1992) and the introduction of Law of Ukraine No. 2849-IX (2023), were designed to combat disinformation and manipulative practices. These regulations addressed emerging challenges in the information space and equipped the state with essential tools to safeguard national interests in the digital domain.

Recognising the global nature of modern information threats, Ukraine has strengthened international cooperation, particularly with the EU and NATO, to counter hybrid challenges. Participation in joint exercises, knowledge exchange, and the development of countermeasures against information attacks have been crucial in enhancing national information security and advancing Ukraine's integration into the international cyber defence system (Jeong *et al.*, 2024). Simultaneously, public diplomacy and strategic communication mechanisms were expanded, including the establishment of the Ukrainian Institute and the increased engagement of diplomatic missions to promote a positive image of Ukraine (Ministry of Foreign Affairs…, 2021). These initiatives sought to foster a favourable international environment and counter information manipulation on a global scale. Despite significant progress in developing political instruments for implementing the information strategy, their effectiveness is often hindered by weak institutional synergy and the absence of a centralised authority in information security. Addressing this challenge remains a priority for Ukraine, necessitating further efforts to optimise information security governance and enhance interagency coordination.

An assessment of Ukraine's information security programs and strategies from 2014 to 2024 presents a mixed record of achievements and challenges. Analysis of the Cybersecurity Strategy of Ukraine 2016-2020 indicates limited effectiveness, with experts estimating that only 40% of the planned objectives were achieved (Decree of the President of Ukraine No. 96/2016, 2016). Despite significant efforts to strengthen Ukraine's cyber defence, several critical tasks remain unfulfilled. An effective mechanism for exchanging information on cyber threats has yet to be established, nor has there been sufficient progress in training qualified specialists or implementing a robust model of public-private sector cooperation. Of particular concern is the underdeveloped cybersecurity research base, which severely limits the ability to address emerging threats.

Despite these challenges, significant progress has been made in strengthening the state's institutional capacity. The establishment of the National Coordination Centre for Cybersecurity under the National Security and Defence Council of Ukraine (Decree of the President of Ukraine No. 47/2017, 2016) and the development of sectoral cyber incident response centres have enhanced Ukraine's ability to address cyber threats. Additionally, the creation of the Centre for Strategic Communications and Information Security (Ministry of Culture and Strategic Communications of Ukraine, 2021) and the implementation of disinformation monitoring and countermeasures have improved the detection and neutralisation of information attacks. These efforts are reflected in international rankings. The National Cyber Security Index (2024) shows Ukraine's significant progress, rising from 25th place in 2020 to 11th in 2023. This highlights the positive trend and Ukraine's increasing role as a key partner in international cybersecurity initiatives, underscored by its active participation in EU and NATO programs. Despite these achievements, the effectiveness of state programs and strategies in information security remains limited by factors such as insufficient funding, a lack of qualified personnel, and inadequate interagency coordination. These issues highlight the need for further development of the national cybersecurity system to effectively address modern information threats.

Based on the analysis, we propose a set of interrelated recommendations for enhancing political instruments to counter hybrid threats in the information sphere. These recommendations focus on establishing a coherent and effective system for safeguarding Ukraine's national interests in the information space. The primary objective is to strengthen coordination and centralise management through the creation of a unified information security coordination centre. This centre should facilitate effective interagency collaboration and a swift response to hybrid threats, addressing existing fragmentation and improving overall effectiveness in countering information threats. Simultaneously, developing an early warning system through a comprehensive monitoring and analysis framework is essential for the timely detection of potential threats and the preparation of preventive measures, crucial in the rapidly evolving information environment. Strengthening the regulatory framework by adopting a comprehensive law on countering hybrid threats is also

necessary to establish a clear legal structure for activities in this area. This law should define the roles and responsibilities of various stakeholders in information security, minimising function overlap and enhancing collaboration between government agencies and the private sector.

Strengthening international cooperation by increasing Ukraine's participation in global cybersecurity initiatives and enhancing information exchange with EU and NATO partners is vital for its integration into the global cyber defence system (Cherleniak & Tokar, 2024). This approach will not only provide access to innovative technologies but also bolster Ukraine's reputation as a reliable ally in combating transnational cyber threats. Establishing an effective public-private cooperation model and enhancing collaboration between government agencies and the business sector in cybersecurity are essential for protecting critical infrastructure and information assets. This requires a structured exchange of threat intelligence and joint development of defence strategies, leveraging the expertise and resources of both sectors to more effectively combat cyber threats.

Enhancing digital and media literacy through a national program is crucial for bolstering society's resilience to information manipulation. This will improve cyber hygiene across the population and cultivate a skilled workforce to combat disinformation and information attacks. Developing a national cyber defence system by investing in Ukrainian cyber defence technologies and training skilled information security professionals is essential for ensuring technological independence and strengthening human resource capacity (Lyndyuk *et al.*, 2023). Enhancing strategic communications through a unified national strategy is crucial to effectively counter disinformation and promote a positive image of Ukraine domestically and internationally. Implementing these interrelated recommendations will establish a comprehensive system for countering hybrid threats in the information sphere, enhancing Ukraine's national security and resilience to contemporary information challenges. To fully understand the dynamics of political instruments and the effectiveness of state programs in Ukraine's information security from 2014 to 2024, it is useful to examine key indicators and their changes over time. Table 1 summarises the main aspects of Ukraine's information security system transformation, highlighting both achievements and challenges.

Table 1. Development dynamics of Ukraine's information security system (2014-2024)

Indicator	2014-2018	2019-2024	Trend
Institutional support	Creation of the MIP	Reorganisation into MCIP, establishment of NCCC	Positive
Legislative framework	Basic laws	Comprehensive upgrade	Positive
International cooperation	Start of active cooperation	Deepening integration	Positive
Countering disinformation	Fragmented measures	Establishment of a CSC, a systematic approach	Positive
National Cyber Security Index rating	25th place (2020)	11th place (2023)	Positive
Implementation of the Cybersecurity Strategy	–	40% (2016-2020)	Moderate
Public-private partnerships	Underdeveloped	At the stage of formation	Moderate
Human resources support	Insufficient	An improvement, but still not enough	Moderate

Note: MIP – Ministry of Information Policy; MCIP – Ministry of Culture and Information Policy; NCCC – National Coordination Centre for Cybersecurity; CSC – Centre for Strategic Communications and Information Security
Source: compiled by the authors

The analysis of the data reveals an overall positive trend in the development of Ukraine's information security system over the past decade. However, despite notable achievements, areas requiring further optimisation remain, including enhancing public-private sector collaboration and improving the efficiency of strategic initiatives. These unresolved issues underscore the need to continue strengthening Ukraine's defence capabilities to counter modern complex information threats, a crucial component for ensuring national stability and establishing a robust national security system, which cannot be achieved without addressing hybrid threats.

Modelling an integrated system of state information policy in the context of hybrid threats. Given the rapid evolution of information technologies and the intensification of hybrid challenges from 2014 to 2024, developing a comprehensive state information strategy is crucial for ensuring national security. This section of the study examines the conceptual framework of information policy, identifies key elements of the information security system, and forecasts its effectiveness under various hybrid threat scenarios. The conceptual model of state information policy in the context of hybrid threats must account for the complex interplay of legal, political, technological, and social factors. Based on an analysis of contemporary approaches to information policy and the specifics of hybrid threats, the following structure is proposed (Table 2).

Table 2. Structure of the conceptual model of the state information policy

Model component	Key elements
Legal and regulatory framework	Constitutional principles of information policy
	Legislative framework in the field of information security
	International agreements and commitments

Table 2, Continued

Model component	Key elements
Institutional architecture	System of public administration bodies in the field of information policy
	Mechanisms for coordination and interaction between different institutions
	Public-private partnership structures
Strategic planning	National Information Security Strategy
	Sectoral and regional information infrastructure development programmes
	Mechanisms for monitoring and evaluating the effectiveness of strategies
Technological infrastructure	Critical infrastructure cyber defence systems
	National cyber threat information exchange platforms
	Technologies for detecting and neutralising disinformation
Human capital	Training system for specialists in the field of information security
	Programmes to improve the digital literacy of the population
	Mechanisms for engaging the expert community
International cooperation	Participation in international cybersecurity organisations and initiatives
	Bilateral and multilateral cooperation agreements
	Mechanisms for sharing experience and technology

Source: created by the authors

The model incorporates recommendations from Ukraine's Draft of the Cybersecurity Strategy (2021-2025), which underscores the importance of developing a national cyber resilience system, fully aligning with the proposed conceptual framework. Based on this model, key elements of the information security architecture can be identified, along with their interdependencies. The central node of this architecture is the Centre for Strategic Management and Coordination, tasked with developing and implementing a unified state information security policy. This body ensures coordination among institutions and facilitates interaction with the business sector and the public. As outlined in the Decree of the President of Ukraine No. 242/2016 "On the National Coordination Centre for Cybersecurity" (2016), these functions are assigned to the National Coordination Centre for Cybersecurity under the National Security and Defence Council of Ukraine.

An early warning system, combining technological monitoring tools, analytical hubs, and rapid response teams, is in place to quickly detect and neutralise threats. The key component of this system is CERT-UA, regulated by Law of Ukraine No. 2163-VIII (2017). The law enforcement and counter-intelligence sectors focus on detecting, preventing, and investigating cybercrime and information sabotage by foreign intelligence services. This responsibility primarily falls to the Security Service of Ukraine and the National Police, whose powers are defined by the Law of Ukraine No. 2229-XII (1992) and Law of Ukraine No. 580-VIII (2015), respectively. The educational and scientific complex plays a crucial role in training specialists, conducting research, and developing innovative technologies in information security.

It includes leading universities, research institutions, and innovation centres. In Ukraine, key institutions in this field include the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", with its specialised cybersecurity programs; Kharkiv National University of Radio Electronics, known for its strong information technology and security programs; and Lviv Polytechnic National University, which houses the Institute of Computer Technology, Automation, and Metrology, training information security specialists. This segment's activities are governed by Law of Ukraine No. 848-VIII (2015). The Strategic Communications System is tasked with formulating and implementing state information policy, countering disinformation, and promoting national interests internationally. The Centre for Strategic Communications and Information Security, established in 2021, plays a central role (Ministry of Culture and Strategic Communications of Ukraine, 2021).

The public-private partnership platform facilitates effective collaboration between the public and private sectors in information security. It includes mechanisms for data exchange, joint training, and the development of security standards. The legal framework for these partnerships is outlined in Law of Ukraine No. 2404-VI (2010). This multi-level structure enables the creation of a comprehensive information protection system that adapts to dynamic changes in the cyber threat landscape and effectively counters contemporary hybrid challenges. The interaction and synergy between the components of the conceptual state information policy model are facilitated through interrelated mechanisms, forming an integrated ecosystem for information space protection. The central element is a unified system for exchanging data on cyber incidents and threats, ensuring the rapid dissemination of critical information across all participants in the information security system.

This system is closely integrated with databases and analytical platforms for in-depth threat analysis and forecasting. The system's effectiveness is reinforced by regular joint exercises and training involving representatives from various agencies, the private sector, and international partners, enhancing preparedness for cyber incidents and fostering a shared understanding of threats. Coordination and strategic decision-making are supported by coordination councils and working groups, which serve as platforms for addressing issues, developing common approaches, and aligning actions within a unified state information security policy.

Together, these elements create a flexible, adaptive, and effective system for countering the evolving landscape of hybrid threats. This system of components and their interrelationships aligns with the recommendations in Information and Analytical Digest No. 7 (July) "Cybersecurity in the Information Society", prepared by the State Scientific Institution Institute of Information, Security, and Law of the National Academy of Legal Sciences of Ukraine and the Vernadsky National Library of Ukraine (Dovgan *et al.*, 2023).

The digest highlights the importance of enhancing coordination among cybersecurity stakeholders and developing public-private partnership mechanisms. To assess the effectiveness of the proposed state information policy model in the context of hybrid threats, three scenarios were analysed, and the system's response to each was predicted (Table 3).

Table 3. Analysis of the information security system response to various hybrid threat scenarios

Aspect	Scenario 1. Large-scale cyberattack	Scenario 2. Long-term information operation	Scenario 3. Technological breakthrough in the field of artificial intelligence
Nature of the threat	Coordinated cyberattack on energy and financial systems, accompanied by disinformation	Systematic spread of disinformation through social media and mass media	Emergence of new types of cyber threats associated with the development of artificial intelligence
Key components of the response	1. Centre for Strategic Management and Coordination. 2. Early detection system. 3. The law enforcement block. 4. Strategic communications system. 5. Public-private partnership platform.	1. Early detection system. 2. Strategic management centre. 3. Educational and scientific complex. 4. Strategic communications system. 5. The law enforcement block.	1. Educational and scientific complex. 2. Strategic management centre. 3. Public-private partnership platform. 4. Early detection system. 5. International cooperation.
Main actions	1. Activation of the crisis protocol. 2. Identification of attack sources. 3. Investigations and international cooperation. 4. Informing the population. 5. Exchange of information with critical infrastructure operators.	1. Identification of disinformation narratives. 2. Developing a long-term strategy. 3. Implementation of media literacy programmes. 4. Campaign to refute fakes. 5. Blocking disinformation networks.	1. Researching new threats. 2. Update the regulatory framework. 3. Cooperation with technology companies. 4. Adaptation of detection algorithms. 5. Development of international safety standards.
Response timeframe	Short-term (hours to days)	Long-term (months to years)	Medium-term (weeks to months)
Efficiency	High	Medium	Moderate
Key challenges	1. Speed of response. 2. Coordination between agencies. 3. Minimising losses.	1. Duration of exposure. 2. Change in public opinion. 3. Identifying hidden sources of disinformation.	1. Technological complexity. 2. The need for significant resources. 3. Adaptation to rapid changes.
Key advantages of the model	Ability to quickly mobilize resources and coordinate actions	A systematic approach to long-term threats	Flexibility and adaptability to new technological challenges
Areas for improvement	Improving the speed of information exchange between agencies	Developing methods for assessing the effectiveness of long-term strategies	Strengthening research capacity and international cooperation

Note: it is important to note that the modelling presented is based on the authors' assessment and reflects potential scenarios of information security system response. These forecasts are hypothetical and require further verification through empirical research and practical testing. The results of the modelling should be considered as a starting point for a more in-depth analysis and discussion among information security professionals. Further research, including quantitative analysis and field experiments, is needed to validate the proposed scenarios and refine the predictions of system effectiveness in different hybrid threat environments
Source: created by the authors

Based on the modelling and analysis of various hybrid threat scenarios, the proposed integrated state information policy system demonstrates strong potential in addressing modern information security challenges. The model is highly effective in responding to acute crises, systematically countering long-term information operations, and adapting to new technological challenges. The analysis also highlighted the need to enhance interagency coordination, develop research capacity, and strengthen international cooperation to effectively address the evolution of hybrid threats. A key success factor is the system's capacity for continuous adaptation, necessitating regular reviews and updates of strategies, technologies, and regulations in response to the evolving information threat landscape. Implementing the proposed model and recommendations for its improvement will significantly enhance the state's information security and resilience to hybrid challenges in the long term.

Discussion

The study identified key aspects of developing and implementing the state information strategy in the context of hybrid challenges. It included a detailed analysis of Ukraine's information policy and security framework, an assessment of political mechanisms for countering hybrid threats, and the proposal of a theoretical model for a comprehensive information policy system. The findings highlight the need for a holistic approach to information security, integrating legal, organisational, technical, and social dimensions. Reviewing Ukraine's legal framework for information security reveals significant progress in legislation from 2014 to 2024, including the adoption of key laws and strategic documents.

Comparisons with the study by S. Kalniete and T. Pildegovičs (2021) showed similar trends in the development of the legal framework at the EU level. The authors stress the importance of a comprehensive legal framework for countering

hybrid threats, aligning with this study's conclusion on the need for a national law on hybrid threats in Ukraine. However, unlike the EU's emphasis on supranational coordination mechanisms, this study focuses on strengthening the national information security system, reflecting Ukraine's unique geopolitical position and the need for rapid response to immediate threats. The study highlighted the need to strengthen coordination among government agencies and establish a centralised decision-making body for information security.

These findings align with M. Wigell's (2021) study, which emphasised the importance of integrated structures to effectively counter hybrid threats. M. Wigell (2021) came up with the idea of "democratic deterrence", which calls for active participation of civil society in fighting hybrid threats. This study's focus on creating partnerships between the government and private sector in information security fits well with this idea. However, unlike the author's focus on foreign policy, this study proposes a more comprehensive approach addressing both internal and external aspects of information policy. An assessment of the effectiveness of political mechanisms for countering hybrid threats identifies shortcomings in the implementation of state initiatives and strategies for information security in Ukraine (Metelskyi & Kravchuk, 2023).

These findings align with C. Tenove's (2020) work on protecting democratic principles from disinformation. C. Tenove (2020) focused on the normative risks of restricting freedom of expression in efforts to combat disinformation. This aligns with the study's findings on the need to balance national security with the preservation of civil rights and freedoms. However, unlike C. Tenove's (2020) focus on social media policy, this study provides a more comprehensive analysis, addressing legislative, institutional, and technological aspects of countering disinformation. This broader perspective offers a deeper understanding of the issue's complexity and supports the development of more effective strategies for protecting the information space.

The conceptual model of the integrated state information policy proposed in this study parallels the approach presented by S. Bondarenko *et al.* (2022), who also stress the need for a systematic approach to strategic national security planning in the context of societal informatisation. However, unlike S. Bondarenko *et al.'s* (2022) focused on technological aspects, this model adopts a more balanced approach, incorporating legal, institutional, and social factors. The study modelled the information security system's response to various hybrid threat scenarios, including a large-scale cyberattack, a prolonged information operation, and a technological breakthrough in artificial intelligence. The analysis revealed that the proposed information policy model is highly effective in responding to acute crises, systematically countering long-term information operations, and adapting to new technological challenges.

Particular attention was given to the scenario of a long-term information operation, involving the systematic spread of disinformation via social networks and media. These findings align with M. Clark's (2020) study on Russian hybrid warfare, which analyses russia's tactics and strategies in information warfare. M. Clark's (2020) emphasises the importance of a systematic approach to countering disinformation and building societal resilience to information manipulation, which is consistent with this study's recommendation for long-term strategies to address information threats. This study offers a broader analysis of hybrid threats, encompassing not only military but also civilian aspects of information security. Unlike M. Clark, who focuses primarily on the military dimension of hybrid warfare, this study also examines the economic, social, and technological aspects. This comprehensive approach enables a more thorough assessment of the impact of hybrid threats on various societal and state sectors, which is particularly relevant given current information challenges.

This study highlights the critical role of innovation in shaping new hybrid threats, particularly through the development of artificial intelligence and quantum computing, which pose new challenges to cyber defence systems. These findings align with P. Kivimaa's (2022) conclusions on the need to transform innovation policy for global security. Author emphasised the development of "safe by design" technologies, which complements this study's recommendations to strengthen research capacity in information security domain. While P. Kivimaa (2022) examined innovation policy primarily in the context of environmental security, this study focuses on the information aspects of national security. Effective responses to technological challenges in information security require not only national efforts but also active international cooperation (Kassymzhanova *et al.*, 2022).

In this regard, the study's findings on the role of international collaboration in countering hybrid threats align with those of M. Weissmann *et al.* (2021). The authors highlighted the importance of international cooperation in countering asymmetric threats, aligning with this study's recommendation to enhance Ukraine's involvement in international cybersecurity initiatives. However, while M. Weissmann *et al.* (2021) focused on international cooperation in the context of military security, this study emphasises the information aspects, including technology and experience exchange in cyber defence. A key element of international cooperation in information security is the harmonisation of regulatory approaches. It is worth paying attention to the study by B. Farrand (2024), which examined the problem of regulating political advertising in the online space. Author proposed the concept of "regulatory mercantilism" in digital policy, which correlates with the findings of this study on the need to improve the legal framework for regulating the information sphere. However, if B. Farrand (2024) focused mainly on the economic aspects of regulation, this study proposes a broader approach, taking into account the security and social aspects of information policy.

This study focused on the impact of hybrid threats on democratic institutions and processes. In the context of analysing the political instruments for the formation and implementation of the state information strategy, it was found that hybrid threats have the potential to significantly undermine trust in state institutions, in particular in the bodies responsible for conducting elections. The study found that information operations can cause a deep split in society, manipulate public opinion, and interfere with electoral procedures, which poses a serious threat to the democratic system as a whole. These conclusions align with and complement the work of H.A. Garnett and T.S. James (2020), who explored the impact of digital technologies on the electoral process.

Their analysis of both the positive and negative aspects of technology in elections supports the comprehensive approach proposed in this study. H.A. Garnett and T.S. James (2020) examined a range of innovations,

including electronic voting systems, voter verification, and tools for predicting election results. Notably, their call for balancing innovation and security in the electoral process aligns with this study's recommendations for an integrated approach to information security. The researchers emphasised the need for flexible regulatory mechanisms that enable the benefits of new technologies while minimising risks to electoral integrity. This approach aligns with our proposed concept of an adaptive information security system, designed to respond effectively to dynamic changes in the information environment.

Comparing this study's results with C. Whyte *et al.* (2021) work on information warfare in the era of cyber conflicts reveals a shared recognition of the complex nature of modern information threats. C. Whyte *et al.* (2021) stressed the need to integrate cybersecurity and information operations, aligning with the integrated information policy system proposed in this study. However, while C. Whyte *et al.* (2021) focused primarily on interstate conflicts, this study offers a broader perspective, incorporating internal aspects of information security. Overall, the study is highly relevant to current scientific discussions on information policy and countering hybrid threats. It provides a comprehensive analysis of the legal and political aspects of information security, considering both Ukraine's national context and global trends. The study's strength lies in its interdisciplinary approach, enabling a multifaceted analysis and the proposal of integrated solutions.

Conclusions

The study successfully identified key areas for improving state information policy in the context of hybrid threats, considering both legal and political aspects. Analysis of contemporary definitions of hybrid threats highlights their complex and multidimensional nature, posing significant challenges to the development of an effective state information policy. Hybrid threats, which integrate traditional and non-traditional warfare methods, present new challenges to national security and sovereignty. Disinformation campaigns, cyberattacks, social media influence operations, and economic pressure through information channels are particularly concerning. An analysis of legal mechanisms for regulating information policy in response to hybrid threats reveals significant progress in Ukraine's legal framework from 2014 to 2024. The adoption of key laws and strategic documents, including Decree of the President of Ukraine No. 47/2017 and the Cybersecurity Strategy, established the foundation for a comprehensive information security system. However, the analysis also identified legislative gaps, such as the limited adaptability of legal norms in a rapidly evolving information landscape and the need for improved interagency coordination mechanisms.

An assessment of the effectiveness of political instruments in shaping and implementing Ukraine's information strategy in the context of hybrid confrontation has revealed significant progress in building institutional capacity to counter information challenges. The establishment of specialised structures, such as the National Coordination Centre for Cybersecurity and the Centre for Strategic Communications, has significantly enhanced the state's ability to identify and neutralise information attacks. The study also highlights the need to enhance interagency cooperation mechanisms and strengthen public-private partnerships in information security. The proposed theoretical model of an integrated information policy system shows significant potential in addressing modern information challenges.

It proves effective in responding to crises, systematically countering long-term information campaigns, and adapting to emerging technological threats. A key success factor is the system's ability to continuously adapt and evolve, necessitating regular updates to strategies, technologies, and regulatory frameworks in response to the dynamic information threat landscape. The study underscores the importance of a comprehensive approach to information security that integrates technical, legal, organisational, and social dimensions. Essential components of an effective information policy include fostering public-private partnerships, strengthening international cooperation, and enhancing digital literacy.

Additionally, prioritising research capacity in information security and adopting innovative technologies are crucial for countering emerging hybrid threats. A key limitation of this study is the absence of empirical data to validate the effectiveness of the proposed theoretical model in real-world conditions. Future research should focus on empirical studies to test theoretical conclusions, the development of quantitative methods for assessing information policy effectiveness against hybrid threats, and an analysis of international strategies for countering emerging information attacks, particularly those involving artificial intelligence. Another crucial area for further investigation is the impact of hybrid threats on democratic processes and the development of mechanisms to safeguard electoral integrity amid information warfare.

Acknowledgements

None.

Conflict of interest

None.

References

[1] Bondarenko, S., Bratko, A., Antonov, V., Kolisnichenko, R., Hubanov, O., & Mysyk, A. (2022). Improving the state system of strategic planning of national security in the context of informatization of society. *Journal of Information Technology Management*, 14, 1-24. doi: 10.22059/jitm.2022.88861.

[2] Bradshaw, S., Bailey, H., & Howard, P.N. (2021). *Industrialized disinformation: 2020 global inventory of organized social media manipulation*. Oxford: Oxford Internet Institute.

[3] Cherleniak, I., & Tokar, M. (2024). Effective governance and the doctrine of "total defence" as factors of state stability in wartime. *Democratic Governance*, 17(1), 5-17. doi: 10.23939/dg2024.05.

[4] Clark, M. (2020). *Russian hybrid warfare*. Washington: Institute for the Study of War.

[5] Cyberattacks on infrastructure: The new geopolitical weapon. (2024). Retrieved from https://www.knowbe4.com/hubfs/Global-Infrastructure-Report-2024_EN_US.pdf.

[6] Davies, J. (2021). *Foreign election interference and hybrid warfare*. Retrieved from https://openworks.wooster.edu/independentstudy/9443/.

[7] Decree of the President of Ukraine No. 242/2016 "On the National Coordination Centre for Cybersecurity". (2016, June). Retrieved from https://zakon.rada.gov.ua/laws/show/242/2016#Text.
[8] Decree of the President of Ukraine No. 447/2021 "On the Decision of the National Security and Defence Council of Ukraine of 14 May 2021 "On the Cybersecurity Strategy of Ukraine". (2021, August). Retrieved from https://zakon.rada.gov.ua/laws/show/447/2021#Text.
[9] Decree of the President of Ukraine No. 449/2014 "On the Decision of the National Security and Defence Council of Ukraine of 28 April 2014 "On Measures to Improve the Formation and Implementation of the State Policy in the Field of Information Security of Ukraine". (2014, May). Retrieved from https://zakon.rada.gov.ua/laws/show/449/2014#Text.
[10] Decree of the President of Ukraine No. 47/2017 "On the Decision of the National Security and Defence Council of Ukraine of 29 December 2016 "On the Doctrine of Information Security of Ukraine". (2016, December). Retrieved from https://www.president.gov.ua/documents/472017-21374.
[11] Decree of the President of Ukraine No. 96/2016 "On the Decision of the National Security and Defense Council of Ukraine dated January 27, 2016 "On the Cyber Security Strategy of Ukraine". (2016, March). Retrieved from https://www.president.gov.ua/documents/962016-19836.
[12] Dovgan, O., Litvinova, L., & Dorohikh, S. (2023). *Cybersecurity in the information society*. Kyiv: Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine.
[13] Draft of the Cybersecurity Strategy of Ukraine (2021-2025). (2021). Retrieved from https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii kyberbezpeki Ukr.pdf.
[14] Executive Order of the President of United States No. 14028 "Improving the Nation's Cybersecurity". (2021, May). Retrieved from https://surl.gd/ssxfay.
[15] Farrand, B. (2024). Regulating misleading political advertising on online platforms: An example of regulatory mercantilism in digital policy. *Policy Studies*, 45(5), 730-749. doi: 10.1080/01442872.2023.2258810.
[16] Galeotti, M. 2018. (Mis)understanding Russia's two "hybrid wars". *Critique and Humanism*, 49, 17-27.
[17] Garnett, H.A., & James, T.S. (2020). Cyber elections in the digital age: Threats and opportunities of technology for electoral integrity. *Election Law Journal: Rules, Politics, and Policy*, 19(2), 111-126. doi: 10.1089/elj.2020.0633.
[18] Ghelani, D. (2022). Cyber security, cyber threats, implications and future perspectives: A review. *Authorea*. doi: 10.22541/au.166385207.73483369/v1.
[19] Hybrid CoE. (2021). *Trend Report 6: The future of cyberspace and hybrid threats*. Retrieved from https://www.hybridcoe.fi/publications/hybrid-coe-trend-report-6-the-future-of-cyberspace-and-hybrid-threats/.
[20] Jeong, M.-J., Rheem, S.-M., Park, Y.-H., Nurtazina, R., & Tkach, M. (2024). Loss and damage of Ukraine's cultural heritage: Actions of the Russian Federation today compared to Germany during World War II. *International Journal of Environmental Studies*, 81(1), 84-92. doi: 10.1080/00207233.2024.2314850.
[21] Joint Communication to the European Parliament and the Council "Joint Framework on Countering Hybrid Threats a European Union Response". (2016, April). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.
[22] Kalniete, S., & Pildegovičs, T. (2021). Strengthening the EU's resilience to hybrid threats. *European View*, 20(1), 23-33. doi: 10.1177/17816858211004648.
[23] Kassymzhanova, A.A., Usseinova, G.R., Baimakhanova, D.M., Ibrayeva, A.S., & Ibrayev, N.S. (2022). Legal framework for external security of the Republic of Kazakhstan. *International Journal of Electronic Security and Digital Forensics*, 14(2), 209-222. doi: 10.1504/IJESDF.2022.121180.
[24] Khorram-Manesh, A., Goniewicz, K., & Burkle Jr, F.M. (2023). Social and healthcare impacts of the Russian-led hybrid war in Ukraine – a conflict with unique global consequences. *Disaster Medicine and Public Health Preparedness*, 17, article number e432. doi: 10.1017/dmp.2023.91.
[25] Kittrie, O.F. (2022). Chinese lawfare in the maritime, aviation, and information technology domains. *Arizona State University Sandra Day O'Connor College of Law Legal Studies*. doi: 10.2139/ssrn.4515674.
[26] Kivimaa, P. (2022). Transforming innovation policy in the context of global security. *Environmental Innovation and Societal Transitions*, 43, 55-61. doi: 10.1016/j.eist.2022.03.005.
[27] Krafft, P.M., & Donovan, J. (2020). Disinformation by design: The use of evidence collages and platform filtering in a media manipulation campaign. *Political Communication*, 37(2), 194-214. doi: 10.1080/10584609.2019.1686094.
[28] Kresina, I.O. (2024). The idea and ideology of national progress. In I.O. Kresina (Ed.), *Strategic priorities of political and legal development of Ukraine in the context of European integration* (pp. 78-79). Kyiv: V. M. Koretsky Institute of State and Law NAS of Ukraine.
[29] Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring Cybersecurity of Ukraine". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2163-19#Text.
[30] Law of Ukraine No. 2229-XII "On the Security Service of Ukraine". (1992, March). Retrieved from https://zakon.rada.gov.ua/laws/show/2229-12#Text.
[31] Law of Ukraine No. 2404-VI "On Public-Private Partnership". (2010, July). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2404-17#Text.
[32] Law of Ukraine No. 2469-VIII "On National Security of Ukraine". (2018, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2469-19#Text.
[33] Law of Ukraine No. 2657-XII "On Information". (1992, October). Reprieved from https://zakon.rada.gov.ua/laws/show/en/2657-12#Text.
[34] Law of Ukraine No. 2849-IX "On Media". (2023, December). Retrieved from https://zakon.rada.gov.ua/laws/show/2849-20#Text.

[35] Law of Ukraine No. 580-VIII "On the National Police". (2015, July). Retrieved from https://zakon.rada.gov.ua/laws/show/580-19#Text.
[36] Law of Ukraine No. 848-VIII "On Scientific and Scientific and Technical Activities". (2015, November). Retrieved from https://zakon.rada.gov.ua/laws/show/en/848-19#Text.
[37] Lyndyuk, A., Boiko, V., Bruh, O., Olishchuk, P., & Rurak, I. (2023). Development of international cooperation of the borderline territorial communities of Ukraine with the EU countries under martial law. *Financial and Credit Activity: Problems of Theory and Practice*, 5(52), 244-255. doi: 10.55643/fcaptp.5.52.2023.4161.
[38] Mälksoo, M. (2020). Countering hybrid warfare as ontological security management: The emerging practices of the EU and NATO. *European Security*, 27(3), 374-392. doi: 10.1080/09662839.2018.1497984.
[39] Metelskyi, I., & Kravchuk, M. (2023). Features of cybercrime and its prevalence in Ukraine. *Law, Policy and Security*, 1(1), 18-25.
[40] Miller, M.L., & Vaccari, C. (2020). Digital threats to democracy: Comparative lessons and possible remedies. *International Journal of Press/Politics*, 25(3), 333-356. doi: 10.1177/1940161220922323.
[41] Ministry of Culture and Strategic Communications of Ukraine. (2021). *The Centre for Strategic Communications and Information Security was presented*. Retrieved from https://www.kmu.gov.ua/news/prezentovano-centr-strategichnih-komunikacij-ta-informacijnoyi-bezpeki.
[42] Ministry of Economic Affairs and Communications of the Republic of Estonia. (2019). *Cybersecurity strategy 2019-2022*. Retrieved from https://www.mkm.ee/media/703/download.
[43] Ministry of Foreign Affairs of Ukraine. (2021). *Public diplomacy strategy of the Ministry of Foreign Affairs of Ukraine 2021-2025*. Retrieved from https://mfa.gov.ua/storage/app/sites/1/%D0%A1%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%97/public-diplomacy-strategy.pdf.
[44] Mishchenko, Kh.O. (2020). *The impact of information technology on mass consciousness in the context of "hybrid warfare"*. Kyiv: National Aviation University.
[45] National Cyber Security Index. (2024). Retrieved from https://ncsi.ega.ee/ncsi-index/?order=-ncsi.
[46] Ördén, H. (2020). Deferring substance: EU policy and the information threat. *Intelligence and National Security*, 34(3), 421-437. doi: 10.1080/02684527.2019.1553706.
[47] Public Law of United States No. 115-278 "Cybersecurity and Infrastructure Security Agency Act". (2018, November). Retrieved from https://www.congress.gov/115/plaws/publ278/PLAW-115publ278.pdf.
[48] Reichborn-Kjennerud, E., & Cullen, P. (2022). *What is hybrid warfare?* Retrieved from https://www.jstor.org/stable/pdf/resrep07978.pdf.
[49] Resolution of the Cabinet of Ministers of Ukraine No. 829 "Some Issues of Optimisation of the System of Central Executive Bodies". (2019, September). Retrieved from https://zakon.rada.gov.ua/laws/show/829-2019-%D0%BF#Text.
[50] Rosenberger, L. (2020). Disinformation disorientation. *Journal of Democracy*, 31(1), 203-207. doi: 10.1353/jod.2020.0017.
[51] Sari, A. (2020). Legal resilience in an era of grey zone conflicts and hybrid threats. *Cambridge Review of International Affairs*, 33(6), 846-867. doi: 10.1080/09557571.2020.1752147.
[52] Schiller, D. (2024). *How to think about information*. Urbana-Champaign: University of Illinois Press.
[53] Tenove, C. (2020). Protecting democracy from disinformation: Normative threats and policy responses. *International Journal of Press/Politics*, 25(3), 517-537. doi: 10.1177/1940161220918740.
[54] Van Raemdonck, N., & Meyer, T. (2024). Why disinformation is here to stay. A socio-technical analysis of disinformation as a hybrid threat. In L. Lonardo (Ed.), *Addressing hybrid threats* (pp. 57-83). Cheltenham: Edward Elgar Publishing. doi: 10.4337/9781802207408.00009.
[55] Vergara Cobos, E.B. (2024). *Cybersecurity economics for emerging markets*. Retrieved from https://policycommons.net/artifacts/16608016/cybersecurity-economics-for-emerging-markets-english/17493164/.
[56] Voropayeva, T., & Averianova, N. (2021). Information and economic security as priority directions of the state policy of Ukraine in the context of the strategy of "smart power". In *Proceedings of the 8th International conference on problems of infocommunications, science and technology* (pp. 197-202). Kharkiv: Institute of Electrical and Electronics Engineers. doi: 10.1109/PICST54195.2021.9772130.
[57] Weissmann, M., Nilsson, N., Palmertz, B., Thunholm, P. (2021). *Hybrid warfare: Security and asymmetric conflict in international relations*. London: Bloomsbury Academic. doi: 10.5040/9781788317795
[58] Whyte, C. (2020). Deepfake news: AI-enabled disinformation as a multi-level public policy challenge. *Journal of Cyber Policy*, 5(2), 199-217. doi: 10.1080/23738871.2020.1797135.
[59] Whyte, C., Thrall, A.T., & Mazanec, B.M. (2021). *Information warfare in the age of cyber conflict*. London: Routledge. doi: 10.4324/9780429470509.
[60] Wigell, M. (2021). Democratic deterrence: How to dissuade hybrid interference. *Washington Quarterly*, 44(1), 49-67. doi: 10.1080/0163660X.2021.1893027.
[61] Zelenov, D. (2024). Psychological mechanisms of influence of disinformation and fake news on the formation of public opinion on Ukrainian European integration: Analysis of Russian propaganda. *Scientific Studios on Social and Political Psychology*, 30(2), 25-35. doi: 10.61727/sssppj/2.2024.25.

Державна інформаційна політика в умовах гібридних загроз: правові та політичні аспекти

Сергій Балан

Кандидат політичних наук, старший науковий співробітник
Інститут держави і права ім. В.М. Корецького НАН України
01601, вул. Трьохсвятительська, 4, м. Київ, Україна
https://orcid.org/0000-0002-9421-7037

Людмила Балан

Директор
ТОВ «Дайв енд Діскавері Рісерч
02000, вул. Костьольна, 8, м. Київ, Україна
https://orcid.org/0009-0008-5819-3323

Вадим Воротинський

Докторант
Інститут держави і права ім. В.М. Корецького НАН України
01601, вул. Трьохсвятительська, 4, м. Київ, Україна
https://orcid.org/0009-0008-2858-9298

Ірина Рибак

Кандидат політичних наук, доцент
Університет «КРОК»
03113, вул. Табірна, 30-32, м. Київ, Україна
https://orcid.org/0000-0002-4165-8154

Володимир Тарасюк

Докторант
Інститут держави і права ім. В.М. Корецького НАН України
01601, вул. Трьохсвятительська, 4, м. Київ, Україна
https://orcid.org/0000-0003-1863-3028

Анотація. Метою дослідження було визначення основних шляхів оптимізації державної інформаційної політики з метою посилення спроможності протистояти складним гібридним викликам. У дослідженні проаналізовано сучасні підходи до визначення гібридних загроз та їх впливу на інформаційну сферу держави. Розглянуто правові механізми регулювання інформаційної політики в контексті протидії гібридним загрозам та оцінено ефективність політичних інструментів формування та реалізації інформаційної стратегії держави в умовах гібридної війни. Аналіз виявив комплексний та багатовимірний характер гібридних загроз, що значно ускладнює процес формування ефективної інформаційної політики. У період з 2014 по 2024 роки нормативно-правова база України у сфері інформаційної безпеки зазнала значного розвитку, але все ще має прогалини, особливо в частині гнучкості правових норм та механізмів міжвідомчої координації. Оцінка ефективності політичних інструментів засвідчила значний прогрес у зміцненні інституційної спроможності України протидіяти інформаційним загрозам, але виявила необхідність подальшого вдосконалення механізмів координації та розвитку державно-приватного партнерства. У дослідженні запропоновано концептуальну модель інтегрованої системи державної інформаційної політики, яка демонструє високу ефективність у реагуванні на різні сценарії гібридних загроз. Ключовим фактором її успіху є здатність системи до постійної адаптації та навчання. Результати дослідження підкреслили необхідність комплексного підходу до забезпечення інформаційної безпеки, що включає правовий, інституційний, технологічний та соціальний виміри. Особливу увагу приділено розвитку дослідницького потенціалу у сфері інформаційної безпеки та впровадженню інноваційних технологій для протидії новим гібридним загрозам. Результати дослідження розширили теоретичне розуміння інформаційної політики в умовах гібридних загроз, що дозволило надати практичні рекомендації щодо вдосконалення відповідних державних стратегій

Ключові слова: національна безпека; кібербезпека; дезінформація; стратегічні комунікації; медіаграмотність; кіберзахист