© Khazar University Press 2023 DOI: 10.5782/.kjhss.2023.51.63

Information Security of the State Under Conditions of Hybrid Warfare: Mechanisms of Ensuring

[1*]Ivan Ablazov; [2]Yevhenii Harkavyi; [3]Sergii Mokliak; [4]Karina Rubel; [5]Volodymyr Smolianiuk

[1,3]Diplomatic Academy of Ukraine named after Hennadii Udovenko, Kyiv, Ukraine
[2]Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
[4]Military Academy named after Yevgeniy Bereznyak, Kyiv, Ukraine
[5]Kyiv National Economic University named after Vadym Hetman, Kyiv, Ukraine
*Corresponding author: ablazov@ukr.net

Abstract

Taking into account the tendencies of democratization and informatization of all sectors of the economy and spheres of public administration, and, accordingly, the increase in information risks, the vast majority of countries in the world today go through a series of stages of ensuring information security. Despite the legislatively established powers of the relevant state authorities and local self-government in this area, the issues of defining their competence and effective interaction are real and effective guarantees of preventing a variety of information threats to national security as in this case effective and timely ways of eliminating existing dangers are provided. Given that large-scale invasions and hybrid wars can cause catastrophic harm and undermine public confidence in the government, the state must make quick decisions. Consequently, establishing an effective mechanism for ensuring information security has become more relevant than ever nowadays. The purpose of the academic paper is to clarify the theoretical fundamentals, as well as the components, directions and other critical practical aspects of the process of ensuring the state's information security under conditions of hybrid warfare. Methodology. In the course of the research, abstraction, idealization, system-structural, comparative, logical-linguistic methods, analysis, synthesis, induction, deduction were used to process scientific information on issues of the state's information security. Results. Based on the research results, the features of the process of ensuring the state's information security in a hybrid war were studied and certain practical aspects of this issue were clarified.

Keywords: Information security, hybrid warfare, protection against illegal information, information security management, information management systems

Introduction

The rapid development of information and communication technologies has led to significant changes in society's life and the transformation of the order of information data exchange. Information has been recognized as an important economic resource in recent decades. The effective organization of information processes contributes to the successful solution of social-economic and political tasks, which significantly increases the profitability of many types of activities. Accordingly, information protection is an extremely important stage in the formation of any country's national security.

The theoretical part of the present research substantiates the concept, essence and components of information security of the state under conditions of hybrid warfare.

The practical part of the research includes determining the most effective measures to ensure effective activities in the state's information security management sphere. These are the most relevant directions of work currently requiring special attention from the perspective of practical applying information security methods, the most important structural elements of the state's information security at the international level, directions for improving the state's information security system under conditions of hybrid warfare. It also comprises the most promising directions of scientific work on issues related to implementing and protecting national interests in the information sphere under conditions of hybrid warfare.

Based on the research results, conclusions were made regarding the issues raised. It was established that the principal measures to ensure effective activity in the state's information security management field are the development and observance of indicators for evaluating the effectiveness of the state's information security protection systems, the implementation of measures to prevent hybrid warfare and counteract its manifestations. The survey showed that the most urgent directions of work requiring special attention from the perspective of practical application of information security methods are identifying internal and external threats to the state's information security and the creating and implementing a surveillance system. At the same time, the most significant structural elements of the state's information security at the international level are information protection and the information-psychological barrier. Along with this, the research revealed the most important areas of improving the state's information security system under conditions of hybrid warfare. These are strategic deterrence, eliminating military conflicts that may arise with the help of information technologies, and forecasting, detection and assessment of information threats. By the way, the respondents singled out the most promising areas of scientific work on issues related to implementing and protecting national interests in the information sphere. These include developing and establishing a long-term program for the creation of an effective information management system based on the latest information technologies, developing interaction between state and commercial information support systems with the aim of more effective using state information resources and ensuring reliable protection of the country's information potential from inappropriate use.

Literature Review

The importance of navigating and effectively working with the flow of information is constantly growing with the transition from an industrial to an information society. The possibilities of the global network, actively used in all spheres of public life, are based on information resources, which are a collection of data in various fields of knowledge and practice. Along with the growth of information's role, the importance of its protection also increases. It is ensured by using information protection tools, which becomes especially relevant during hybrid warfare (Weissmann et al., 2021), (Eberle & Daniel, 2021).

A system-structural approach is frequently applied in scientific studies of numerous aspects of national security, including information security, as it allows for considering security provision at multiple levels of its system or mechanism of provision. Such a prevalence of this approach in legal scientific studies is probably due to the already established doctrine of the legal regulation's mechanism, the state administration mechanism, the mechanism of law enforcement, etc. (Ott, 2021), (Tkachenko & Diadin, 2022).

Information security mechanisms provide for organizing state institutions' activities and civil society's structures. It also involves implementing practical measures, levers, incentives, methods of action to identify and organize (attract) the necessary material, spiritual, personnel resources, integrating society's various spheres to ensure the fulfillment of information security goals (Raimundo &Rosário, 2022).

The efficiency of protecting state information as a whole is ensured by the effectiveness of each component of the state mechanism, consisting of interconnected elements, namely:

– a set of state institutions participating in the process of formation and implementation of the information security policy, that is, the institutional mechanism for ensuring information security;

- a set of roles and relations, which includes legal relations arising during the implementation of the information security policy and specific roles, forms and methods of activity of this policy's subjects;
- a hierarchical set of legal norms and principles regulating the content and process of information security policy implementation, that is, the legal mechanism for ensuring information security (Mumford &Carlucci, 2022), (Zvezdova & Vakalyuk, 2022), (Weissmann, 2019).

An information security system is an internal structure, a systematized whole, unity, interconnection and differentiation of its individual elements (object, subjects, main characteristics, protection levels and a list of threats) (Frizon, 2022).

Aims

The purpose of the research is to clarify the standpoint of specialists in the field of information security in state bodies and scientists conducting research activities in this sphere regarding the features of the process of ensuring information security during hybrid warfare.

Materials and Methods

The study of modern tendencies in practical implementing state information security mechanisms under conditions of hybrid warfare was conducted by means of a questionnaire survey of 218 information security specialists and 92 scientists conducting scientific activities in the Chernivtsi, Volyn, Rivne, and Kyiv regions of Ukraine. The research was conducted using the Survio service.

Results

The survey participants believe that currently, in the conditions of rapid informatization of all public life's spheres and, accordingly, an increase in the danger of information risks, the main measures to ensure effective activities in the field of the state's information security management are as follows (Figure 1):

- development and observance of performance indicators for state information security protection systems;
- implementing measures to prevent hybrid war;

- countering manifestations of information war.

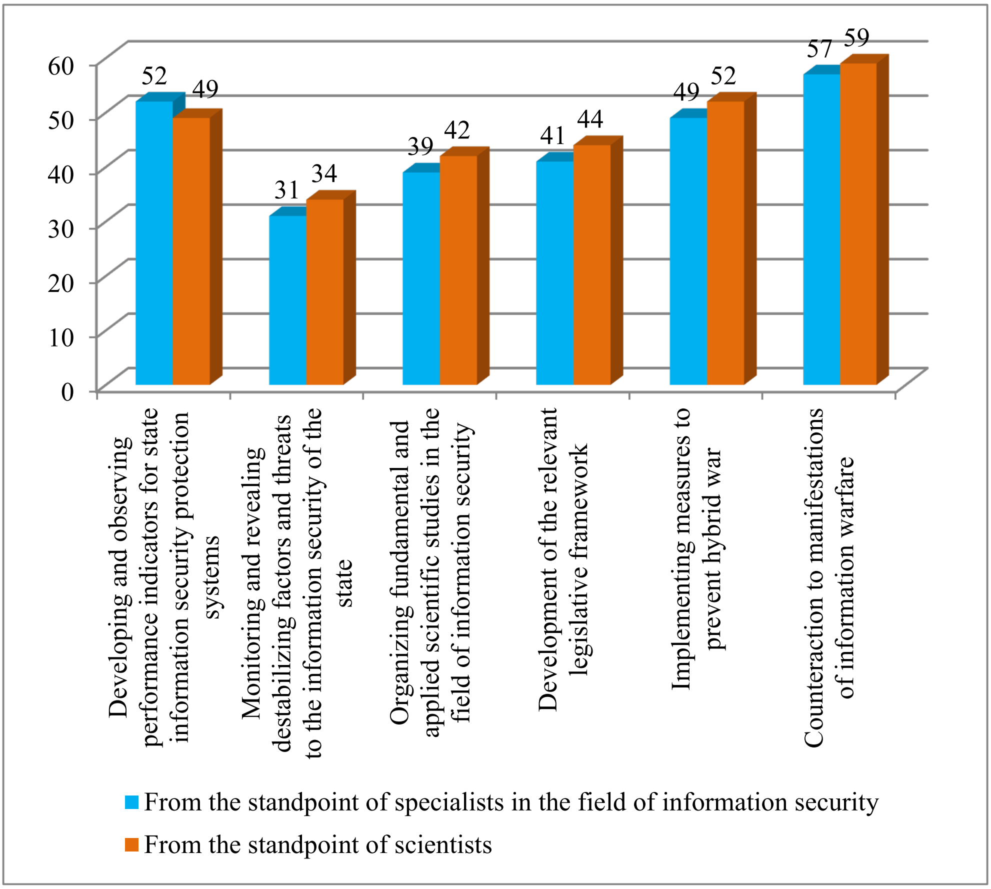

Figure 1. The primary most effective measures on ensuring effective activities in the field of state information security management, %

Source: compiled by the authors.

During the survey, the respondents identified the following most relevant directions of work requiring special attention from the perspective of the practical application of the methods to ensure information security in the state (Figure 2).

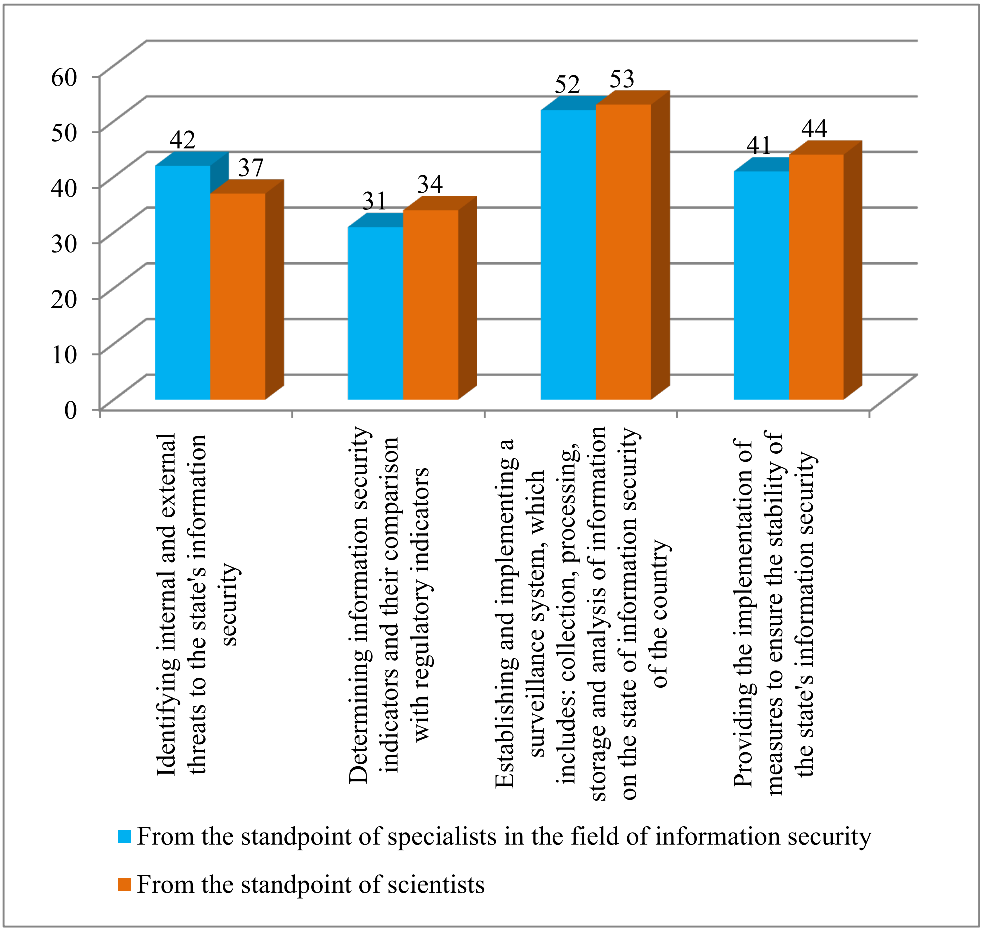

Figure 2. Directions of work currently requiring special attention from the perspective of the practical application of the methods to ensure information security in the state, %

Source: compiled by the authors.

The key directions that the information security mechanism should perform include identifying internal and external threats to the state's information security, and establishing and implementing a surveillance system, which comprises: monitoring, collection, processing, storage and analysis of information on the state of information security of the country.

The survey made it possible to establish the most important structural elements of the state's information security at the international level (Figure 3).

It can be observed from Figure 3 that the most important structural elements of information security at the international level include the information protection containing state or commercial secrets and the information and psychological barrier, which provides for the implementation of a system of measures aimed at protecting against a targeted impact on the victim of an attack, his mental state or image at the international level.

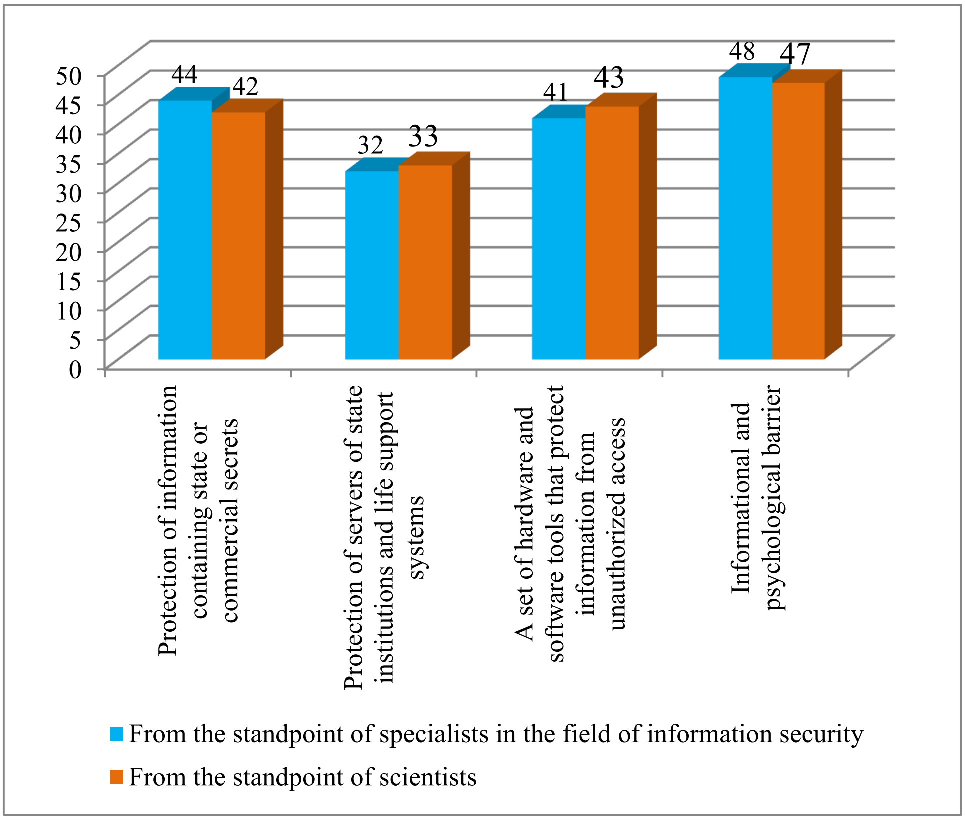

Figure 3. The most important structural elements of the state's information security at the international level, %.

Source: compiled by the authors.

During the research, the respondents were asked to identify the most important directions for improving the state information security system under conditions of hybrid warfare (Figure 4).

According to the respondents' standpoint, the main directions of improving the information security system nowadays are strategic deterrence and elimination of military conflicts that may arise with the help of information technologies and forecasting, detection and assessment of security threats, including information.

The survey participants also determined the most promising directions of scientific work on issues related to implementing and protecting national interests in the information sphere, which, will be especially in demand in the future (Figure 5).

The survey showed that such directions are as follows: the development and adoption of a long-term program for establishing an effective information management system based on the latest information technologies, the development of interaction between state and commercial information support systems with the aim of more effective use of state information resources and ensuring reliable protection of the country's information potential from inappropriate use.

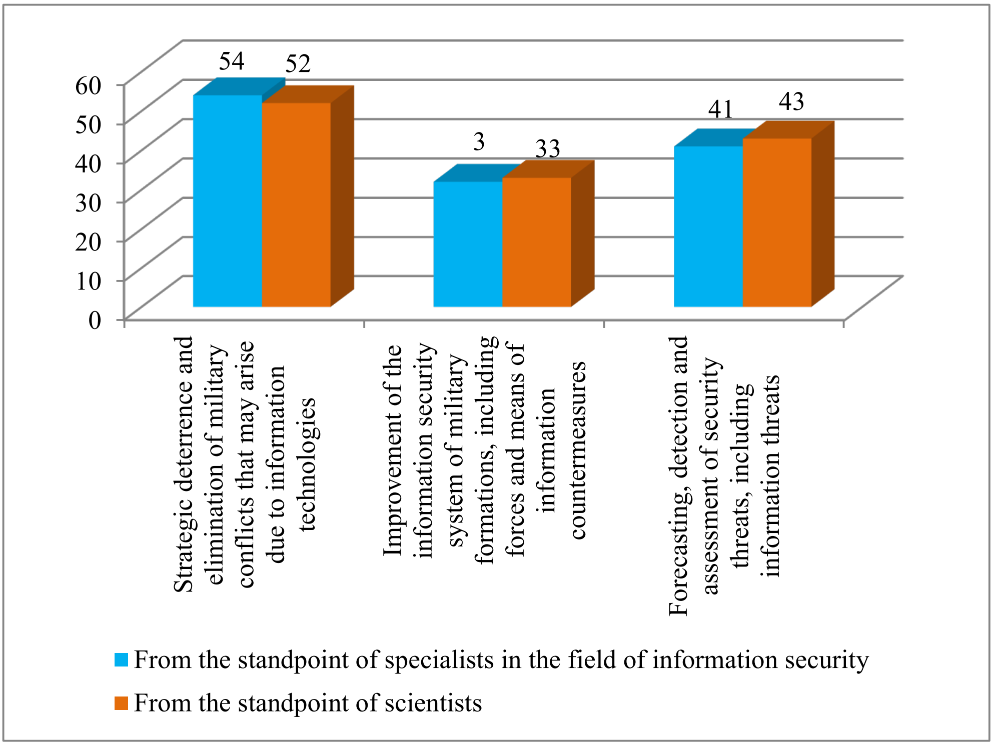

Figure 4. The most important directions for improving the state information security system under conditions of hybrid warfare, %.

Source: compiled by the authors.

Discussion

Unfortunately, the formation of the global information society could not prevent wars as a means of resolving political, economic, territorial, ethnic, religious and other conflicts. In addition, the processes of introducing modern information and communication, social-political and social-psychological technologies have made these wars more sophisticated and insidious (Smolianiuk, 2018), (Loishyn et al., 2021).

In conditions of information wars, social organisms (state, political, social institutions and organizations) are destroyed. The civilizational and cultural code of the nation and social morality are deformed, the sense of patriotism is destroyed, and the human psyche is shaken. The ability of people to resist enemy attacks is impaired (Loishyn, 2022), (Kresin, 2022).

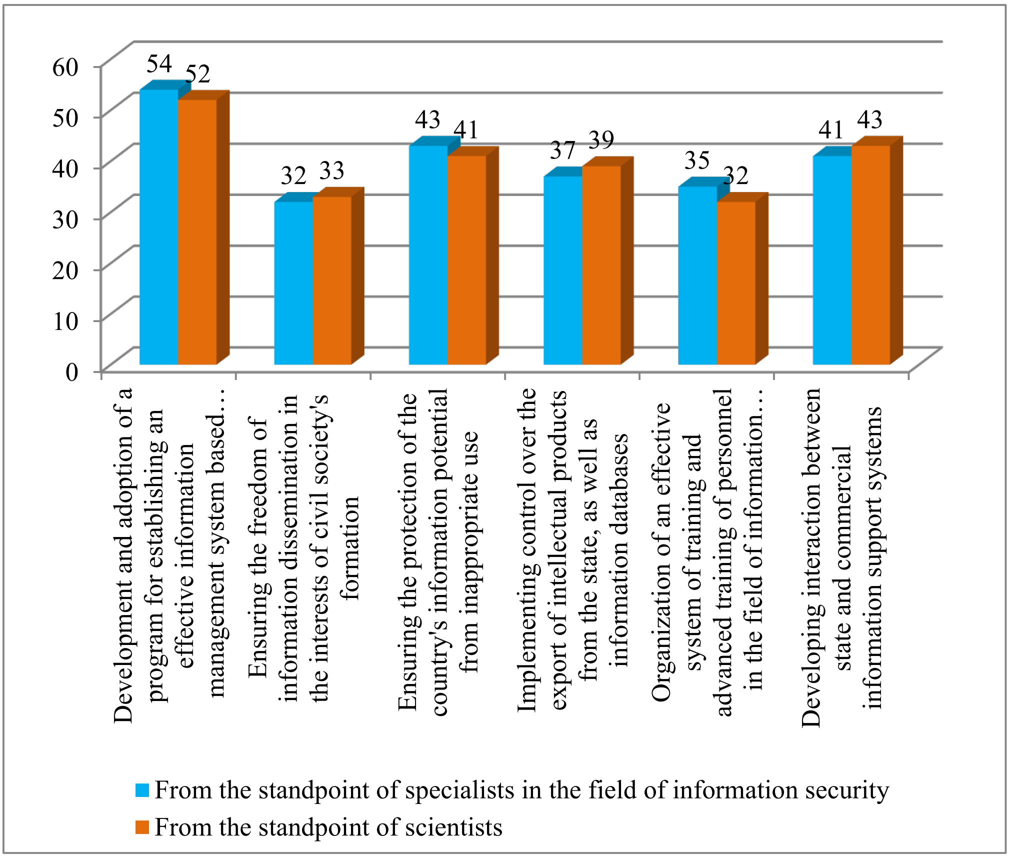

Figure 5. The most promising directions of scientific work on issues related to implementing and protecting national interests in the information sphere under conditions of hybrid warfare, %.

Source: compiled by the authors.

The dominance of information factors in conducting hybrid wars is defined by the information society's essence, which, according to its ideologues, is determined by the qualitative transition of human civilization from the agrarian-industrial to the information phase of development, when communication resources become much more important than society's material and technical resources (Johnson, 2018).

According to this basic philosophical construction, the enemy actively uses social structures in the conditions of information and hybrid warfare. These structures significantly influence the world and national public consciousness of countries that have become the object of an information attack. These are as follows: means of mass communication: radio broadcasting, cable, satellite television and radio, mobile video, audio and Internet communications, multimedia social networks, websites, printed and electronic newspapers, magazines and books; religious, cultural, trade union, environmental, human rights, journalistic and other public organizations; diplomatic structures (Jacuch, 2022), (Nilsson et al., 2021).

In conditions of hybrid warfare, when the country has become the object of an attack and is exposed to a significant number of information threats, their elimination requires the adoption of certain organizational and legal measures. The strategic goal of ensuring information security as a national security component is determined by the country's national interests in the domestic political sphere, which include the preservation of the constitutional order, the maintenance of national harmony and the legal space's unity (Wan &Raju, 2022), (Mazaraki, Kalyuzhna & Sarkisian, 2021).

Information security is a complex, dynamic, integral social system, the components of which are the security subsystems of the individual, the state and society. It is an interdependent system information unit of the latter, constituting a qualitative determination aimed at protecting the vital interests of a person, society and the state, ensuring their competitive, progressive development (Mačák, 2021).

Ensuring information security through the consistent implementation of a well-formulated national information strategy can be important for the state's success. It will contribute to solving tasks in the political, military-political, military, social, economic and other spheres of state activity. The implementation of a successful information policy can significantly affect the resolution of internal, external and military conflicts (Kostyuk&Brantly, 2022).

Conclusions

Therefore, the analysis of the scientific literature on the research topic and the questionnaire results showed that, in general, information security policy as a social phenomenon has a complex nature. It includes domestic and foreign political, economic, technological, military and other elements and, consequently, requires a comprehensive approach to its studying. The state authorities' activities should be aimed at implementing specific tasks in this area. They should be united by the single goal of creating relevant conditions for implementing the country's information security. The state information security system is an integral part of the overall national security system of the country. It is a set of state bodies, non-state structures and citizens that must coordinate information security activities on the basis of uniform legal norms, effectively resisting information threats in modern conditions.

References

Eberle, J. & Daniel, J. (2021). Anxiety geopolitics: Hybrid warfare, civilisational geopolitics, and the Janus-faced politics of anxiety. Political Geography, 92, Januar 2022, 102502 https://www.sciencedirect.com/science/article/abs/pii/S0962629821001621. https://doi.org/10.1016/j.polgeo.2021.1

Frizon, G.(2022). Global Hybrid warfare. November 2022. Project: Hybrid warfare. https://www.researchgate.net/publication/365149402_Global_Hybrid_warfare

Jacuch, A.(2022). Countering hybrid threats: resilience in the eu and strategies. August 2020.The Copernicus Journal of Political Studies. https://www.researchgate.net/publication/346385699_COUNTERING_HYBRID_THREATS_RESILIENCE_IN_THE_EU_AND_NATO'S_STRATEGIES https://doi.org/10.12775/CJPS.2020.001.

Johnson,R.(2018). Hybrid War and Its Countermeasures: A Critique of the Literature. Small Wars and Insurgencies, 29, 1, 141-163. https://www.researchgate.net/publication/322017964_Hybrid_War_and_Its_Countermeasures_A_Critique_of_the_Literature https://doi.org/10.1080/09592318.2018.1404770.

Kostyuk, N. & Brantly, A. (2022).War in the borderland through cyberspace: Limits of defending Ukraine through interstate cooperation. Contemporary Security Policy, 43, 3, 498-515. https://www.researchgate.net/publication/362969497_War_in_the_borderland_through_cyberspace_Limits_of_defending_Ukraine_through_interstate_cooperation https://doi.org/10.1080/13523260.2022.2093587.

Kresin,O.(2022). Counteracting hybrid threats in Ukrainian legislation. Foreign·trade:· economics,·finance,·law, 120, 1, 4–17. http://journals.knute.edu.ua/foreign-trade/article/view/7. https://doi.org/10.31617/zt.knute.2022(120)01

Loishyn, A. (2022). Analysis of generations of wars according to the concepts of technological and wave development of society. Journal of Scientific Papers "Social Development and Security", 12, 2, 1-13. https://paperssds.eu/index.php/JSPSDS/article/view/435. https://doi.org/10.33445/sds.2022.12.2.1.

Loishyn, A., Tkach, I., Tkach, M. & Shevchuk, V. (2021). Analysis and systematization of approaches to understanding the concept of "hybrid war". Journal of Scientific Papers «Social Development and Security», 11, 1, 145-162. https://paperssds.eu/index.php/JSPSDS/article/view/291. https://doi.org/10.33445/sds.2021.11.1.15

Mačák, K.(2021). Unblurring the lines: military cyber operations and international law. Journal of Cyber Policy, 6, 1, 1-18. https://www.researchgate.net/publication/357031006_Unblurring_the_lines_military_cyber_operations_and_international_law https://doi.org/10.1080/23738871.2021.2014919

Mazaraki, A., Kalyuzhna, N. & Sarkisian, L. (2021). Multiplicative Effects Of Hybrid Threats: This work was supported by the National Research Foundation of Ukraine [grant number 2020.02/0245]. (Scientific fair "Support for research of leading and young scientists") within project Trade and economic policy of country in the conditions of hybrid war&quotю Baltic Journal of Economic Studies, 7(4), 136-144. http://baltijapublishing.lv/index.php/issue/article/view/1269. https://doi.org/10.30525/2256-0742/2021-7-4-136-144

Mumford, A. &Carlucci, P. (2022). Hybrid warfare: The continuation of ambiguity by other means. 17 June 2022. European Journal of International Security, 1, 1–15. https://www.cambridge.org/core/journals/european-journal-of-international-security/article/abs/hybrid-warfare-the-continuation-of-ambiguity-by-other-means/1B3336D8109D418F89D732EB98B774E5. DOI: https://doi.org/10.1017/eis.2022.19.

Nilsson, N., Weissmann, M., Palmertz, B.&Thunholm, P. January (2021). Security challenges in the grey zone: Hybrid threats and hybrid warfare in book: Hybrid Warfare. https://www.researchgate.net/publication/349495446_Security_challenges_in_the_grey_zone_Hybrid_threats_and_hybrid_warfare. https://doi.org/10.5040/9781788317795.0005.

Ott, C. (2021). The new offensive cyber security: Strategically using asymmetrical tactics to promote information security Received (in revised form). Cyber Security: A Peer-Reviewed Journal, 5, 4 286–293. Henry Stewart Publications, 2398-5100. https://www.rothwellfigg.com/media/publication/15025_Cyber%20Security%20Journal_Ott_2022.pdf.

Raimundo, R., J. &Rosário, A.T.(2022). Cybersecurity in the Internet of Things in Industrial Management. Applied Sciences, 2022, 12, 3, 1598. https://www.mdpi.com/2076-3417/12/3/1598 https://doi.org/10.3390/app12031598.

Smolianiuk, V.F. (2018). Systemic principles of national security of Ukraine. Bulletin of Yaroslav Mudryi National Law University. Series: Philosophy, philosophy of law, political science, sociology, 2, 37, 107-126. https://doi.org/10.21564/2075-7190.37.133543.

Tkachenko, S.O. & Diadin, A.S. (2022). Public safety in the conditions of martial law and mental warfare, Law and Safety, 86, 3, 128-139. https://doi.org/10.32631/pb.2022.3.11. http://pb.univd.edu.ua/index.php/PB/article/view/612.

Wan, W. &Raju, N. (2022). Strategic Instability Across Domains. November 2022. https://www.researchgate.net/publication/365739529_Strategic_Instability_Across_Domains.

Weissmann, M. (2019). Hybrid warfare and hybrid threats today and tomorrow: towards an analytical framework.June 2019. Project: Hybrid Threats and Warfare. https://www.researchgate.net/publication/334967002_Hybrid_warfare_and_hybrid_threats_today_and_tomorrow_towards_an_analytical_framework https://doi.org/10.2478/jobs-2019-0002.

Weissmann, M., Nilsson, N., Palmertz, B. & Thunholm P. (2021). Hybrid Warfare: Security and Asymmetric Conflict in International Relations, https://www.researchgate.net/publication/349497596_Hybrid_Warfare_Security_and_Asymmetric_Conflict_in_International_Relations. https://doi.org/10.5040/9781788317795

Zvezdova, O., & Vakalyuk, A. (2022). Cyber security strategy in hybrid war. Acta De Historia & Politica: Saeculum XXI, 03, 82-90. https://ahpsxxi.org/index.php/journal/article/view/51/ https://doi.org/10.26693/ahpsxxi2021-2022.03.082