DOI: https://doi.org/10.34069/AI/2023.69.09.7

How to Cite:

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

State information security strategies in conditions of hybrid threats

Стратегії інформаційної безпеки держави в умовах гібридних загроз

Received: August 9, 2023 Accepted: September 16, 2023

Written by:

Anton Khriapynskyi[1]
https://orcid.org/0000-0002-2492-051X

Ihor Khmyrov[2]
https://orcid.org/0000-0002-7958-463X

Ivo Svoboda[3]
https://orcid.org/0000-0002-0941-4686

Mykhailo Shevchuk[4]
https://orcid.org/0000-0001-7549-6344

Vira Iastrebova[5]
https://orcid.org/0000-0002-0757-2090

Abstract

Hybrid information threats under the conditions of modern development of digital technologies are currently becoming one of the major issues for a modern democracy. The amount of damage that hybrid threats bring to the world economy contributes to the establishment of effective legal mechanisms to combat them. The purpose of the study was to single out the information security strategies under conditions of hybrid threats, including the spread of disinformation and fake news. The application of the comparative analysis method mad it possible to identify the gaps in information security strategies for countering hybrid threats. The strategy of information security in the conditions of hybrid threats is a coordinated action plan aimed at countering and fighting hybrid threats to safeguard cyberspace and preserve a democracy. Information security against hybrid threats is based on such cornerstones as: availability, confidentiality, integrity of information data, and safety. Enhancement of information security under the conditions of hybrid threats should be carried out at the expense of digital

Анотація

Гібридні інформаційні загрози за умов сучасного розвитку цифрових технологій стають однією із основних проблем для демократичного суспільства. Обсяг шкоди, яку гібридні загрози приносять світовій економіці, сприяє встановленню ефективних правових механізмів для їх боротьби. Метою дослідження був визначення стратегій інформаційної безпеки за умови гібридних загроз, включаючи розповсюдження дезінформації та фейкових новин. Шляхом використання методу компаративного аналізу з'ясовано прогалини стратегій інформаційної безпеки щодо протидії гібридним загрозам. Стратегія інформаційної безпеки в умовах гібридних загроз є скоординованим планом дій, спрямованих на протидію та боротьбу з гібридними загрозами з метою захисту кіберпростору та збереження демократичного суспільства. Інформаційна безпека з протидії гібридним загрозам базується на таких принципах, як: доступність, конфіденційність, цілісність інформаційних даних та безпечність. Удосконалення інформаційної безпеки за умов

[1] Candidate of Law, Director, "KHRIAPYNSKYI & CO" LTD, Kharkiv, Ukraine.

[2] Doctor of Science in Public Administration, Associate Professor, Senior Researcher, Scientific Department of Problems of Civil Protection and Technogenic and Ecological Safety of the Scientific and Research Center, National University of Civil Protection of Ukraine, Kharkiv, Ukraine. WoS Researcher ID: CZO-2061-2022

[3] Associate Professor, Guarantor of Security Management Studies, AMBIS, a.s. University, Prague, Czech Republic. WoS Researcher ID: CBV-4475-2022

[4] Candidate of Science of Law, Doctoral Student, Department of Constitutional Law, Administrative Law, Financial Law, Leonid Yuzkov Khmelnytskyi University of Management and Law, Khmelnytskyi, Ukraine. WoS Researcher ID: IQW-6294-2023

[5] Post Graduate Student of the 1st Year, Department of Political Theories, National University "Odesa Law Academy", Odesa, Ukraine.

transformation, increasing the level of digital literacy of society and establishing a fair responsibility measure for a purposeful spreading of disinformation. The perspective of further research is addressing information security strategies as well as elaborating practical guidelines for the formation of a secure information space.

Keywords: information security, threat, strategy, cyberspace, disinformation.

гібридних загроз слід здійснювати за рахунок цифрової трансформації, збільшення рівня цифрової грамотності суспільства та встановлення справедливої міри відповідальності за умисне розповсюдження дезінформації. Стратегії інформаційної безпеки вбачаються в подальшому дослідженні та обґрунтуванні з метою визначення практичних рекомендацій щодо формування безпечного інформаційного простору.

Ключові слова: інформаційна безпека, загроза, стратегія, кіберпростір, дезінформація.

Introduction

In 2014, the open Russian conflict with Ukraine became an external threat for many countries, as a rapid flow of disinformation, Russian propaganda and fake news began occurring in their information space. Ignoring such an information flow of false information can entail social destabilization with subsequent manifestation of violence, riots and crimes against the pillars of national security. Taking into consideration the need to create an effective system of discerning disinformation and deterring its spread, in particular the one that poses a threat to national security, the search for effective information security strategies becomes a priority for a number of states worldwide.

The relevance of the research topic under study is due to the fact that today's challenges create numerous external threats to the functioning of secure information space. Their volume and variety is rapidly changing and gaining momentum. An uncontrolled, systematic and ongoing flow of such information is one of the principal issues that threaten the country’s national sovereignty. Taking into account the internal and external vectors of information dissemination in cyberspace, representatives of the international community are taking individual (first) steps in the direction of legal regulation of the dissemination of information, procedures for restricting access in the event that it becomes biased and unreliable (fake) and contains calls for violation of national interests of the state. At the same time, the initial steps are being taken to develop legal mechanisms for bringing to justice subjects involved in the spread of disinformation and fake news. A legal mechanism of punishment for the untimely implementation of appropriate response measures by both competent state bodies and private entities is also being elaborated.

The purpose of the current study is to examine the information security strategies of the world's leading countries and their countermeasures against hybrid information threats.

To address the specified purpose of the article, the following research objectives were set forth:

- to determine the content of the information policy and its functioning measures by analyzing the scientific literature;
- to conduct an analysis of the international legal treaties’ provisions and the norms of the national legislation of the EU countries in the field of information security and to determine the legal mechanisms for countering hybrid threats;
- to analyze the current state of information security strategies’ efficiency while tackling the hybrid threats of the EU member states and to establish the ways in enhancing thereof.

Literature Review

Probing into the EU information legislation through the lens of hybrid threats, Lonardo (2021: 1077) and Khmel (2022: 92-93) argue that EU policy puts the main responsibility for countering hybrid threats on EU member states, i.e. at the national level, not at the regional level. The same viewpoint is maintained by Pijpers et al., (2021), examining NATO and EU cyberspace security measures against hybrid threats. In scholar’s opinion, EU information security does not depend on regional mechanisms for countering hybrid threats, but rather on NATO's mandate as a indispensable partner in military and other frameworks of deterrence against hybrid threats. Being a full NATO’s partner, the EU exercises the right to military assistance in the event of extraordinary threats to the national security of a NATO member state. On the other hand, threats in cyberspace area are not qualified as such to which physical force must be applied, and assistance is beyond the scope of classical military powers. Probing into the issue of legal regulation of the information sphere in the EU, Datzer and Lonardo (2022: 2-3) claims that hybrid threats are external threats posing a threat to national security. Another scholar, Saurwein and Spencer-Smith (2020: 8254), while conducting an analysis of the impact of hybrid threats on the development of the information sphere, notes that the effectiveness of the information strategy will depend on the establishment of legal countermeasures against false news in cyberspace. One of these measures is the developers' provision of safe digital content on the Internet. Addressing information security strategies, Li et al., (2020: 192) and Alraja et al., (2023) maintain that Internet users' perception and awareness entails more efforts by the producers of digital software to ensure information security in cyberspace as well as on part of the government officials to create a balance between producers and users by introducing effective measures to develop the applicable policy of information security. According to Nord et al., (2020: 218-219) and Xue et al., (2021: 2-4), information security strategies should evaluate and take into account the level of users' legal awareness, their digital literacy and self-efficacy in ensuring information security.

As noted by Sari (2018) and Perot (2019: 40-43), countering hybrid threats in cyberspace is necessary by strengthening the legal basis of information policy and promoting one's vision of international order. According to Tenove (2020: 517-519) and Allcott et al., (2019: 2-3), the development of information policy in a legal state should include legal measures aimed at ensuring information security and legal mechanisms for the protection of the information space, based on international information standards. The combination of these information policy components will evidently contribute to countering threats in the information sphere.

Analyzing information security as a component of Taiwan's innovative development, Wu et al., (2020) concludes that information security in the era of the Internet is a strategic factor for the development of artificial intelligence and the development of a smart cities network in Taiwan. To ensure technological development of Taiwan, the government constantly adjusts the information security strategy, which ensures the proper functioning of innovative programs in cyberspace. The analysis of promising ways of improving the system of information security measures in such smart cities is implemented by studying the relationships between the formulation, implementation, support and effectiveness of the information security policy, support and effectiveness of the information security policy.

Bajarūnas (2020: 62-64) and Kalniete and Pildegovičs (2021: 24-25) conducted the analysis of information security strategies in the EU and means of combating hybrid threats. The result of which was the statement that under modern conditions, after Russia's unprovoked open military invasion of Ukraine in 2014, countering hybrid threats and disinformation became a priority task for the EU. The introduction of universal and effective means of ensuring information security is a complex process. Due to the rapid changes occurring, external and internal threats in cyberspace take place requiring ongoing monitoring and updating the means of countering them. Investigating information security strategies in the Czech Republic under the conditions of external threats, Daniel and Eberle (2021: 432) notes that the means of combating hybrid information warfare should be based on proper defense, timely response, high level of education and media literacy, and effective protection methods. Datsenko (2019: 40-41) and Panchenko (2021: 29) presented their findings of probing into the means of ensuring information security through the prism of combating Russian propaganda in the information space of Ukraine. These were to the point of asserting the feasibility of introducing interconnected means of countering hybrid threats in cyberspace. According to the scholars, cooperation with international organizations, exchange of experience with leading countries in terms of information security strategies, monitoring of media resources, transparency of the work of competent authorities on information policy and public participation in the socio-political life of the state will sufficiently contribute to the creation of safe content in the information space (Semenyshyn et al., 2020).

That being said, despite quite a wide-ranging scholarly research on the above issue, questions regarding the effectiveness of state information security strategies through the prism of hybrid threats and war, which determines the relevance of the current research topic, remain scarce.

Methods and Materials

The analysis procedure of the current research included three stages. At the first stage, a review of the scientific literature was carried out into the subject of hybrid threats significance and their implications for a democratic society, as well as the possibilities for cyberspace and social networks to shape society's behavior. A review of the scientific literature was also conducted on the research subject in terms of information security measures, the improvement strategy and operation principles thereof. The provisions' selection of the EU countries' international and national legislation in the field of information security against hybrid threats was carried out. The materials of the leading organizations have been selected to assess the countries' rating regarding their capabilities to protect information in cyberspace.

At the second stage, theoretical and experimental research was conducted by comparing the obtained results and analyzing discrepancies. The provisions of the Convention on Cybercrime for determining the grounds and punishment measure for committing criminal acts in cyberspace have been considered. The provisions of the Action Plan against Disinformation were considered for the purpose of evaluating information security strategies for countering hybrid threats and the effectiveness of its measures in hybrid warfare. Furthermore, the provisions of the ISO/IEC 27000 series of international standards for the assessment of information security in hybrid warfare were also studied. A review of the national legislation in the field of information security of France, Germany, Poland, and Great Britain was carried out to determine the state of establishment of effective mechanisms for countering hybrid threats. By comparing the Global Cybersecurity Index 2020, National Cyber Security Index 2022 and Cyber Defense Index 2022/23 ratings, the current state of EU countries' cyber defense strategies is highlighted.

At the third stage, using the functionality of Microsoft Office software, the criteria for assessing the level of cyber protection of the EU countries were systematized, as well as the scientific discussion on the effectiveness of information security strategies in the fight against hybrid threats and ways to improve them. By means of the specified software product, an analysis of the processed materials was carried out on the subject of the assigned tasks and the findings of the conducted research were drawn into a report.

The application of comparative analysis method, scientific, legal, statistical and practical information about hybrid threats and their implications for a democratic state were analyzed. The cyber protection level of each EU country was evaluated relying on the system-logical method. Owing to the combination of empirical and theoretical methods, an empirical interpretation of the theory and theoretical interpretation of empirical data was conducted, while also considering the legal principles of countermeasures and the fight against hybrid threats in the information space were distinguished. The doctrinal analysis of scientific works on the problematic issues of ensuring information security under the conditions of hybrid threats made it possible to identify gaps in information security strategies and find the measures to bridge them.

Taking into consideration the study objectives, the sample was as follows: general characteristics of information security and its relevance for the state; determination of the principles of information security under the conditions of hybrid threats; perceiving the information space as a digital platform for spreading misinformation and threats to national security; the system of international and national legislation of the EU countries in the field of ensuring information security; the system of legal measures against hybrid threats; assessment of cyber protection level of EU member states; national legislation of France, Germany, Poland, Great Britain in the field of combating and combating disinformation; the hands-on practice of combating hybrid threats. The comprehensive character of studying these objects contributed to the identification of information security strategies' through the prism of countering and combating hybrid threats in current social environment.

The principal materials on which the research was grounded are provisions of international documents as follows: Convention on Cybercrime, EU Action Plan against Disinformation and a series of international standards ISO/IEC 27000. Besides, there are provisions of national legislation of EU countries, namely: Code of Practice for Countering Disinformation on the Internet and Netzwerkdurchsetzungsgesetz (Deutschland), Law in the field of combating information manipulation (France), Anti-fake law (Great Britain). Furthermore, the research was carried out drawing on the practice of the joint unit of Great Britain with Poland for countering Russian disinformation and propaganda, and then the analysis was conducted into the data of the Global Cybersecurity Index 2020, National Cyber Security Index 2022 and Cyber Defense Index 2022/23 rankings. Consequently, the study of the selected research was carried out on the basis of scientific literature on information security and doctrinal analysis on the problems of combating hybrid threats.

Results

The gaps analysis in the field of information legislation indicates an imbalance and unevenness between measures to ensure the functioning of information policy and information security protection (Figure 1).

Enhancing information security in cyberspace should be carried out by upgrading digital transformation as the major factor in the digitalization development of state authorities. This position is held by 87% of respondents included in the Global Cybersecurity Index 2020 (International Telecommunication Union, 2021). Similarly, (87%) heads of the organization and managerial directors point to the feasibility of improving legal mechanisms for countering and fighting hybrid information threats. What is more, unauthorized access to a large amount of personal and confidential information, which is transmitted by electronic means, is likely to cause serious consequences. In 2020, the amount of losses due to cybercrime was estimated at 1 trillion US dollars, and in 2021 - almost 6 trillion US dollars (International Telecommunication Union, 2021). The said scale of losses from hybrid information threats testifies to the need to improve legal mechanisms for countering fake news and disinformation. In sum, the security of information and the creation of safe digital content is currently becoming a prerrequisite for the information society development.

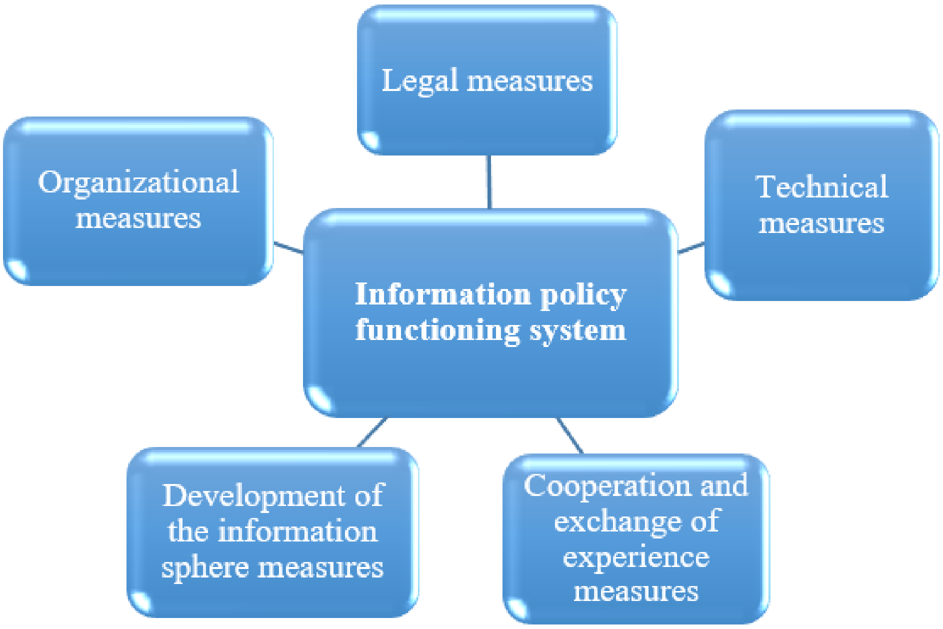
Legal measures
Organizational measures
Technical measures
Information policy functioning system
Development of the information sphere measures
Cooperation and exchange of experience measures

Figure 1. System of measures aimed at ensuring information security
Source: Author's own development.

Time and again, European countries suffered negative consequences from external information threats. Accordingly, they quickly began to introduce means of countering such threats by improving legal mechanisms for regulating the information sphere. The level of information protection in cyberspace and the state of secure Internet content in the EU are indicated in Table 1. The level of information security of EU member states is examined by assessing the date of Global Cybersecurity Index 2020, National Cyber Security Index 2022 and Cyber Defense Index 2022/23 for each EU country individually.

Table 1.
Level of cyber protection of EU member states

Country	Global Cybersecurity Index 2020		Country	National Cyber Security Index 2022			Country	Cyber Defense Index 2022/23	
	Rating	Indicator		Rating	National Cyber Security Index	The level of digital development		Rating	Indicator
Great Britain	2	99.54	Belgium	1	94.81	74.07	Netherlands	2	7.61
Estonia	3	99.48	Lithuania	2	93.51	67.34	Poland	6	6.91
Spain	4	98.52	Estonia	3	93.51	75.59	Great Britain	7	6.79
France	9	97.6	Czech Republic	4	92.21	69.21	France	8	6.78
Germany	13	97.41	Germany	5	90.91	69.21	Switzerland	10	6.45
Portugal	14	97.32	Romania	6	89.61	59.84	Italy	11	6.37
Latvia	15	97.28	Greece	7	89.61	64.02	Germany	13	6.24
Netherlands	16	97.05	Portugal	8	89.61	68.46	Spain	14	6.13
Norway	17	96.89	Great Britain	9	89.61	79.96			
Belgium	19	96.25	Spain	10	88.31	72.21			
Italy	20	96.13	Poland	11	87.01	65.03			
Finland	22	95.78	Austria	12	85.71	75.76			
Sweden	26	94.55	Finland	13	85.71	78.35			
Greece	28	93.98	France	15	84.42	77.29			
Austria	29	93.89	Sweden	16	84.42	81.51			
Poland	30	93.86	Denmark	17	84.42	82.68			
Denmark	32	92.6	Croatia	18	83.12	64.63			
Croatia	33	92.53	Slovakia	19	83.12	65.44			
Slovakia	34	92.36	Netherlands	20	83.12	81.86			
Hungary	35	91.28	Italy	23	79.22	67.26			
Cyprus	41	88.82	Latvia	25	75.32	66.23			
Switzerland	42	86.97	Ireland	26	75.32	75.18			
Ireland	46	85.86	Switzerland	27	75.32	82.93			
Iceland	58	79.81	Bulgaria	28	74.03	62.06			
Romania	62	76.29	Hungary	36	67.53	64.25			
Slovenia	67	74.93	Norway	38	67.53	80.19			
Czech Republic	68	74.37	Cyprus	39	66.23	68.83			
Bulgaria	77	67.38	Slovenia	56	59.74	69.74			

Source: Author's own development based on (International Telecommunication Union, 2021; MIT Technology Review, 2023; NCSI, 2023).

In 2018, the EU aimed to protect a democratic society and ensure the public's right to free access to a wide variety of verified information in order to form citizens' own political views in the future. In other words, to ensure a free and fair electoral process through the participation of citizens in political debates with the free expression of personal position, the European Commission approved the Action Plan against Disinformation (European Commission, 2018). Drawing on the said Plan, the EU outlined four main areas of information security strategies for countering and combating disinformation: improving the mechanism for detecting hybrid threats in cyberspace; coordinated and timely response to the detected flow of false information that poses a threat to the foundations of national security; safety of digital platforms and social networks; raising awareness and supporting citizens. The plan defines the principle measures to combat disinformation. In particular, these are as follows: ongoing careful monitoring of the information flow in cyberspace for threats to the security of using digital platforms; creation of a system of rapid notification in case of detection of a flow of fake news containing a threat to the national interests of the state; enhancing the level of digital technologies used in the fight against disinformation and increasing the level of digital media literacy of staff who take measures to counter disinformation.

Being fully aware of the rapid development of digital technologies and their fast adaptation in the life of a person and the state, the international community approved the Convention on Cybercrime in 2001 in order to protect information that is promptly spreading in cyberspace (Council of Europe, 2001). This Concept not only defines the importance of information for a present-day digital society and digital state power, but most importantly establishes the measure of punishment - criminal liability for committing crimes in the digital space and for intentionally spreading disinformation with the aim of threatening the national interests of the state.

On the other hand, realizing the risks from hybrid information threats for a democratic state, the EU countries have started building their own national information security strategies aimed at combating hybrid threats. Thus, in order to stop fake information in social networks, Germany adopted the Law "On the Regulation of Social Networks" (Netzwerkdurchsetzungsgesetz) and the Code of practice for combating misinformation on the Internet. In order to combat external information threats, France adopted the Law on combating information manipulation, which introduced a mechanism for state monitoring and control of the information flow in social networks. The establishment of legal instruments for combating hybrid threats in cyberspace also took place in Great Britain through the adoption of the Anti-Fake Law. In order to counter the flow of Russian propaganda and false information, Great Britain together with Poland formed a unit to counter Russian disinformation and propaganda. Russia's open aggression against Ukraine compels the whole glabal community to quickly find legal mechanisms to counter external informational threats.

Yet another way to tackle hybrid threats in the information space is the international standards of the information security management system. The ISO/IEC 27000 series of standards is a guideline and practical provision for the hands-on application of the necessary means, strategies, principles to ensure information security (organization, firm, government body, etc.). Moreover, those apply to provisions and approaches to risk management from hybrid information threats. The ISO/IEC 27000 series also contains provisions on taking practical actions aimed at overcoming information security threats, provisions on the level of professional training of personnel authorized to carry out anti-disinformation measures, as well as the level of digital technologies utilized to protect cyberspace, organizational resources and users.

The effectiveness of the information security strategy for overcoming hybrid threats in cyberspace will depend on the legal mechanism for implementing the principles on which it relies (Figure 2). The system of these principles reflects the entire spectrum of human rights and freedoms, the observance of which is a priority for every democratic state governed by the rule of law.

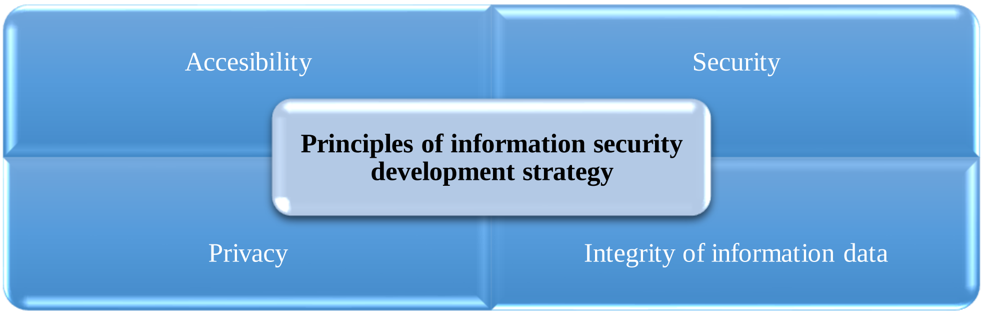
Accesibility
Security
Principles of information security development strategy
Privacy
Integrity of information data

Figure 2. The principles of information security
Source: Author's own development.

Discussion

The rapid development of digital technologies contributed not only to the development of the information sphere, but also became a platform for an uncontrolled flow of false information that undermines the basis of national security. Currently, countering hybrid information threats in cyberspace is becoming a priority task for the majority of countries worldwide. That being said, under the conditions of digital platforms' and social networks' safe use, it is expedient to safeguard the fundamental human right to free expression of views as well as the right to obtain information and freely use it.

According to Lonardo (2021: 1076), hybrid threats are measures of diplomatic, military, economic or technological tactics to destabilize a political opponent. Bajarūnas (2020: 62) maintains that combating hybrid threats is a constant, never-ending process that requires technological development of society, increasing the level of media literacy of the public, political stability and the introduction of effective information security strategies. Information security under modern conditions of hybrid information warfare requires effective strategies for the development of information policy from states, while its effectiveness depends on society's digital literacy level as well as the development of the state (Daniel & Eberle, 2021: 432; Weissmann, 2019: 18-19). The same viewpoint is shared by Datsenko (2019: 40-41) and Panchenko (2021: 29), who believe that the information security strategy should include the following measures: constant monitoring of media resources; publication of analytical studies' findings; society's undisputed participation in social and political life of the state through their work in state authorities; continuous cooperation with international organizations and other principal states aimed at sharing leading experience in combating hybrid threats in the information space and developing unified measures to counter fake news, propaganda and disinformation. The combination of these measures will contribute to the creation of safe content on the Internet.

Cyber threats in the digital information space are not characterized as threats that require physical effort to overcome them (Pijpers et al., 2021). Basically, hybrid threats in the information space are alarming to the integrity of the EU. Therefore, after Russia's open invasion on the territory of Ukraine, as noted by Datzer and Lonardo (2022: 2-3) and Dziundziuk et al., (2022), the EU actively began to develop new information strategies to overcome disinformation from false Russian propaganda in the EU's information space.

The overriding characteristic of EU information strategies is that they must establish countermeasures against hybrid threats in the information space throughout the EU (that is, at the regional level). Hence, in practice, measures of information strategies are uneven throughout the EU. Due to the fact that some member states insist on strengthening the regulation of digital platforms, while others stand firm on weakening the protection of liability and strengthening the compulsion to create safe content in the Internet (George et al., 2021: 1067-1069; Saurwein & Spencer-Smith, 2020: 825).

Freedman et al., (2021: 38-39) and Bajwa (2021: 16-18) note that that uncontrolled hybrid threats as well as ignoring the scale of their consequences become the cause of civil society destabilization by way of leaking the fake information with anti-Semitic and anti-democratic implications through civilian information spaces, doing that with the aim of committing riots or crimes against the national security interests of the state. In such cases, ensuring information security is a strategic task for any economically developed country, and it is made possible only provided that the threats are eliminated in the information space (Allcott et al., 2019: 2; Tenove, 2020: 518).

As a result of the doctrinal analysis of the specified problems of the effectiveness of strategies for the development of information policy and ensuring information security for the purpose of overcoming hybrid threats, gives us the ground to note that scholars see the expediency in probing deeper into information security and its measures of support, which generally adjusts the scope and perspectives of safeguarding the interests of national security.

Conclusions

The information security strategy for countering and combating hybrid threats is a general action plan aimed at counteracting hybrid threats in the information space, the implementation of which is established for a certain period. The system of measures aimed at ensuring information security consists of legal, technical, organizational measures as well as cooperation and experience exchange activities and measures for the development of the information sphere. Enhancing information security in cyberspace under the conditions of hybrid threats is possible by upgrading digital transformation, improving the level of digital literacy of society, establishing a fair measure of punishment for committing cybercrimes. The effectiveness of the information security strategy under the conditions of hybrid threats will depend on the level of implementation of the principles which it is built on (availability, confidentiality, integrity of information data, safety).

The prospect of further research is to elaborate practical guidelines for enhancing the field of information security by improving legal mechanisms aimed at combating hybrid threats. Therefore, we see a further perspective in the empirically researched and theoretical and methodological substantiation of effective mechanisms for countering hybrid threats as the main obstacle to the creation of safe digital content for users to express in the digital space their own free views. Accordingly, the obtained research results can be used in elaborating certain mechanisms for improving information security strategies.

Bibliographic references

Allcott, H., Gentzkow, M., & Yu, C. (2019). Trends in the diffusion of misinformation on social media. *Research & Politics*, *6*(2), 1-8. https://doi.org/10.1177/2053168019848554

Alraja, M. N., Butt, U. J., & Abbod, M. (2023). Information security policies compliance in a global setting: An employee's perspective. *Computers & Security*, 129, 103208. https://doi.org/10.1016/j.cose.2023.103208

Bajarūnas, E. (2020). Addressing hybrid threats: Priorities for the EU in 2020 and beyond. *European View*, 19(1), 62-70. https://doi.org/10.1177/1781685820912041

Bajwa, A. (2021). Information disorder, the Triumvirate, and COVID-19: How media outlets, foreign state intrusion, and the far-right diaspora drive the COVID-19 anti-vaccination movement. *The Journal of Intelligence, Conflict, and Warfare*, 4(2), 16-45. https://doi.org/10.21810/jicw.v4i2.3067

Council of Europe. (2001). *Convention on Cybercrime (ETS No. 185)*. Budapest 23/11/2001. https://acortar.link/uRQcKm

Daniel, J., & Eberle, J. (2021). Speaking of hybrid warfare: Multiple narratives and differing expertise in the 'hybrid warfare'debate in Czechia. *Cooperation and Conflict*, 56(4), 432-453. Doi: 10.1177/00108367211000799

Datsenko, A. Yu. (2019). Strategic directions of struggle against Russian propaganda and disinformation in the information space of Ukraine. *Gilea: Scientific Bulletin*, 145(3), 39-43. (In Ukranian)

Datzer, V., & Lonardo, L. (2022). Genesis and evolution of EU anti disinformation policy: entrepreneurship and political opportunism in the regulation of digital technology. *Journal of European Integration*, 1-16. https://doi.org/10.1080/07036337.2022.2150842

Dziundziuk, V., Krutii, O., Sobol, R., Kotukova, T., & Kotukov, O. (2022). Improved Planning of Information Policy in the Cyber Security Sphere under Conditions of Hybrid Threats. *Cuestiones Políticas*, 40(74).

European Commission. (2018). *Action Plan against Disinformation*. Brussels, 5.12.2018 JOIN(2018), 36. https://digital-strategy.ec.europa.eu/en/library/action-plan-against-disinformation

Freedman, J., Gjørv, G. H., & Razakamaharavo, V. (2021). Identity, stability, Hybrid Threats and Disinformation. *ICONO 14, Revista de comunicación y tecnologías emergentes*, 19(1), 38-69. https://doi.org/10.7195/ri14.v19i1.1618

George, J., Gerhart, N., & Torres, R. (2021). Uncovering the Truth about Fake News: A Research Model Grounded in Multi-Disciplinary Literature. *Journal of Management Information Systems* 38(4), 1067-1094. https://doi.org/10.1080/07421222.2021.1990608

International Telecommunication Union. (2021). *Global Cybersecurity Index 2020*. ITUPublications. https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2021-pdf-e.pdf

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

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

Li, Y., Pan, T., & Zhang, N. (2020). From hindrance to challenge: How employees understand and respond to information security policies. *Journal of enterprise information management*, 33(1), 191-213.

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

MIT Technology Review. (2023). *The Cyber Defense Index 2022/23*. Retrieved from https://technologyreview.com/2022/11/15/1063189/the-cyber-defense-index-2022-23/

NCSI. (2023). *National Cyber Security Index 2022*. Retrieved from https://ncsi.ega.ee/ncsi-index/?order=rank

Nord, J. H., Koohang, A., Floyd, K., & Paliszkiewicz, J. (2020). Impact of habits on information security policy compliance. *Issues in Information Systems*, 21(3), 217-226. https://doi.org/10.48009/3_iis_2020_217-226

Panchenko, O. (2021). Institutional support for the processes of counteraction to Russian information expansion and propaganda in the modern world. *Information and Law*, 3(38), 28-34. https://doi.org/10.37750/2616-6798.2021.3(38).243797

Perot, E. (2019). The art of commitments: NATO, the EU, and the interplay between law and politics within Europe's collective defence architecture. *European security*, 28(1), 40-65.

Pijpers, P. B., Boddens Hosang, J. F. R., & Ducheine, P. A. (2021). Collective Cyber Defence the EU and NATO Perspective on Cyber Attacks. *Amsterdam Law School Research Paper, (2021-37)*. http://dx.doi.org/10.2139/ssrn.3962163

Sari, A. (2018). Blurred lines: hybrid threats and the politics of international law. *Strategic Analysis, The European Centre of Excellence for Countering Hybrid Threats*. Retrieved from https://ssrn.com/abstract=3164265

Saurwein, F., & Spencer-Smith, C. (2020). Combating Disinformation on Social Media: Multilevel Governance and Distributed Accountability in Europe. *Digital Journalism,* 8(6), 820-841. http://dx.doi.org/10.1080/21670811.2020.1765401

Semenyshyn, M., Hryshchenko, I., Alekseieva, K., Oliinyk, V., & Buha, H. (2020). Research of features of professional self-actualization of civil servants through the determinants of information security. *Revista San Gregorio*, 42, 41-52. Retrieved from https://acortar.link/3YyT4N

Tenove, C. (2020). Protecting Democracy from Disinformation: Normative Threats and Policy Responses. *The International Journal of Press/Politics*, 25(3), 517-537. https://doi.org/10.1177/1940161220918740

Weissmann, M. (2019). Hybrid warfare and hybrid threats today and tomorrow: towards an analytical framework. *Journal on Baltic Security*, 5(1), 17-26.

Wu, Y. C., Sun, R., & Wu, Y. J. (2020). Smart city development in Taiwan: From the perspective of the information security policy. *Sustainability*, 12(7), 2916. https://doi.org/10.3390/su12072916

Xue, B., Warkentin, M., Mutchler, L. A., & Balozian, P. (2021). Self-efficacy in information security: a replication study. *Journal of Computer Information Systems*, 1-10. https://doi.org/10.1080/08874417.2021.2015725