UDC 34:004; 347
DOI: 10.32518/sals2.2025.276

Соціально-правові студії. 2025. Т. 8, № 2
Social & Legal Studios. 2025. Vol. 8, No. 2

Information law in the context of information aggression

Leontiy Chystokletov
Doctor of Law, Professor
Lviv Polytechnic National University
79005, 1/3 Kniazia Romana Str., Lviv, Ukraine
https://orcid.org/0000-0002-3306-1593

Yurii Nazar
Doctor of Law, Professor
Lviv State University of Internal Affairs
79000, 26 Horodotska Str., Lviv, Ukraine
https://orcid.org/0000-0002-8059-4413

Oleksandra Khytra
Doctor of law, Professor
Lviv State University of Internal Affairs
79000, 26 Horodotska Str., Lviv, Ukraine
https://orcid.org/0000-0002-3632-5101

Dmytro Zabzaliuk
Doctor of Law, Professor
Lviv State University of Internal Affairs
79007, 26 Horodotska Str., Lviv, Ukraine
https://orcid.org/0000-0002-1041-0148

Yulia Komissarchuk
PhD in Law, Associate Professor
Lviv State University of Internal Affairs
79007, 26 Horodotska Str., Lviv, Ukraine
https://orcid.org/0000-0002-5079-334X

Abstract. The issues of information law in the context of hybrid warfare, which includes issues of cybersecurity, countering disinformation, protecting information sovereignty and freedom of speech, have become particularly relevant and one of the key areas of legal research in response to large-scale information aggression against Ukraine. The purpose of the study was to investigate the regulator's response to external factors in the form of hybrid information warfare. The research used methods of comparative analysis, a systematic approach, and a formal logical method. The study analysed key aspects of the functioning of information law under martial law, in particular, its ability to ensure freedom of speech and access to reliable information. The legal mechanisms that ensure information security were investigated, considering the latest forms of information aggression, including cyber threats, propaganda, disinformation, and manipulation in social networks. The practice of international cooperation in the field of information security was summarised and it was established that effective counteraction to hybrid warfare requires adaptation of the legal environment to the conditions of the latest information and communication technologies. Contemporary legislative initiatives in Ukraine in the field of information security were analysed and ways to improve national information legislation were proposed, in particular, in the areas of cybersecurity, personal data protection, countering fakes, and regulating media activities. The practical value of the study lies in the possibility of using its results by legislators, law

Suggested Citation **Article's History**: Received: 18.02.2025 Revised: 01.05.2025 Accepted: 25.06.2025

Chystokletov, L., Nazar, Yu., Khytra, O., Zabzaliuk, D., & Komissarchuk, Yu. (2025). Information law in the context of information aggression. *Social & Legal Studios*, 8(2), 276-284. doi: 10.32518/sals2.2025.276.

*Corresponding author

enforcement agencies, researchers and specialists in the field of cybersecurity to develop and implement an effective information policy in the context of a military conflict

Keywords: information security; digital environment; cyber threats; freedom of expression; legal regulation; information manipulation

Introduction

The relevance of the study is conditioned by the unprecedented increase in the scale and impact of information threats that accompany armed conflicts. As of 2025, the issue of legal response to targeted information attacks was becoming critical not only for the security of the state, but also for preserving the democratic foundations of society. Countering hostile manipulation, cyber threats, and attempts to destabilise through the media requires flexible and timely legal solutions. In the context of the intensive spread of digital technologies and increasing external pressure on the state's information space, legal regulation in this area cannot remain secondary. One of the most serious challenges for information freedom in a hybrid war is the spread of disinformation and fake news, which are actively used as tools of influence. In times of war, especially in the context of information aggression, media and digital platforms become channels for manipulating public opinion, spreading false facts, and creating so-called "alternative realities". This hinders the development of objective opinion, which is the basis of a democratic society. In Ukraine, as in many other countries, disinformation is becoming part of not only military strategies, but also social processes that undermine the morale of the population and their trust in government institutions. It is important that the fight against fakes and manipulation requires not only technological means, but also a clear legal framework that would ensure a balance between controlling the information space and protecting the right to freedom of expression. The study of this issue is necessary for the development of mechanisms that can effectively protect national interests in the new conditions of hybrid confrontation.

The contemporary information world, saturated with technological innovations and unexpected changes on the geopolitical front, has witnessed serious challenges, in particular, hybrid warfare, which is a real test for national and international security. The Russian-Ukrainian confrontation reflects new forms and methods of military operations, where information aggression and cyber-attacks are becoming integral components of modern warfare (Chmyr *et al.*, 2023).

In the scientific literature, the problem of legal support of information security in the context of hybrid warfare has been widely discussed. I. Sopilko *et al.* (2022) focused on the threats of information wars as a challenge to national security, noting that the state needs to update the legal means of protecting the information space. In turn, N. Nuritdinov (2024) and D. Vedeneyev (2021) analysed the impact of critical thinking on the level of information stability of citizens, emphasising the role of education and information hygiene as elements of the legal mechanism for countering disinformation.

S. Fedoniuk *et al.* (2023) investigated the specific features of information security policy development in Ukraine during the war, concluding that the existing regulatory framework is fragmented and requires significant updating. A. Pravdiuk (2022; 2023) noted the need for a comprehensive reform of legislation in the field of cybersecurity based on international standards. In this context, A. Khriapynskyi (2024) also stressed that national legislation is not sufficiently adapted to the hybrid nature of contemporary conflicts, and S. Saeed *et al.* (2023) pointed out the need to unify legal regulation

How these changes should be implemented was investigated by T. Berezyovets (2020), emphasising that legal instruments should not only respond, but also prevent threats. T. Hurzhi (2019) focused on the intersectoral nature of information law in countering hybrid threats, especially in aspects of interaction between the public and private sectors. Zh. Denisyuk (2021) analysed in detail the forms of information attacks and proposed ways of legal response, considering international experience. A. Brantly (2022), who investigated Ukraine's cyber defence strategies, stressed the importance of adapting legal solutions to the dynamic conditions of hybrid conflict. L. Kormych *et al.* (2024) considered digital transformation as a key factor influencing the development of the legal field in the field of information security.

The purpose of this study was to critically evaluate the transformations already carried out by the legislator in the field of information law from the standpoint of their effectiveness and compliance with contemporary challenges, and to substantiate legal mechanisms that can ensure an appropriate level of information security in the context of the rapid development of digital technologies and the globalisation of the information space. The focus was on both changes in national legislation and trends in international legal regulation in the field of information protection, in particular, in the context of the growing number of cyber threats, disinformation, and violations of privacy rights. Thus, the objectives of the study were a comprehensive assessment of the legal regulation of the information space, analysis of mechanisms for implementing information rights and obligations of subjects of legal relations, identification of existing gaps and conflicts in legislation, and search for areas for its improvement. Special attention was paid to the issues of balancing security and freedom of speech, and the introduction of new legal instruments that consider the dynamics of information technology development and the transformation of the nature of threats in the cyber sphere.

Materials and methods

The study used an interdisciplinary approach that combined elements of legal science, information security, political science, and social communications. The theoretical framework of the study was the concept of information sovereignty, supplemented by the doctrine of hybrid warfare, in which information aggression was considered as a component of asymmetric conflicts. Among the concepts of such confrontation, the idea of cosciential warfare, which includes encroachments on cultural heritage and information symbols of statehood, was particularly useful, which is also associated with the norms on the return of cultural property to their countries of origin (UN General Assembly Resolution No. 48/15, 1993). The term "coscientiality" comes from the Latin word *conscientia* – consciousness or conscience. That is

why special attention in the study was paid to legal mechanisms that can protect the legal and national consciousness, intellectual centres that are responsible for development, in accordance with H. Zadorozhny's (2021), "national survival strategies". The provisions of the theory of human rights in the context of restrictions on freedom of speech during a state of emergency or martial law were also considered.

From a methodological standpoint, the study was based on a combination of several classical methods of legal science. In particular, the system-analytical method helped to identify relationships between regulatory legal acts, international agreements, and mechanisms for responding to information threats. It was applied in the analysis of the current legislation of Ukraine in the field of information security and its comparison with the relevant international standards. The comparative legal method helped to compare Ukrainian legislation with the practices of the EU and NATO countries, in particular, in terms of regulatory response to hybrid attacks. As a result, a number of fundamental differences were identified, including potential areas for adapting national law. The doctrinal method was used to investigate the views of researchers regarding the legal content of information security, the limits of freedom of speech during the war, and legal restrictions in cyberspace. Within the framework of this method, the terms "information aggression", "information weapons", and "hybrid attack" were analysed.

The studied legislation included such regulatory acts as: Law of Ukraine No. 2657-XII "On Information" (1992), Law of Ukraine No. 2849-IX "On Media" (2022), and Decree of the President of Ukraine No. 152/2022 "On the Unified Information Policy in Wartime" (2022). The impact of such fundamental documents as the European Convention on Human Rights (1950) and the United Nations General Assembly Resolutions No. A/70/174 (2015) and No. A/RES/76/19 (2021) was considered, which form the basic principles of states' behaviour in the digital environment. This indicates that the source base was characterised by its regulatory diversity, allowing to develop a comprehensive picture of the legal response to information threats in the context of hybrid warfare and to ensure the validity of conclusions based on a multi-level legal reality.

Results and Discussion

Analysis of the impact of information aggression and cyber threats on the legal system of Ukraine in the context of the Russian-Ukrainian war requires focusing on practical aspects of the functioning of information law (Lysenko *et al.*, 2023). In this context, it is appropriate to recall the opinion of T. Hurzhi (2018), who emphasised that hybrid warfare comprehensively transforms public relations, covering the political, economic, and information spheres, and also affects the functioning of state institutions. Such changes, in his opinion, require a prompt legal response from the national legal system, since it is the quality and speed of this response that largely determine the effectiveness of countering new challenges. Therefore, the development of effective legal mechanisms in the field of information security is not only desirable, but also a necessary element of the national sustainability strategy.

From the standpoint of information law, it is important to consider hybrid warfare as an important context for the development and improvement of legal mechanisms, in which information law, with the help of information and legal support tools regulated by information and legal norms, appears as one of the main levers of countering information aggression, cyber threats, and other aspects of hybrid warfare. Special attention in this process should be focused on the need to study and improve the legal framework governing information security and citizens' rights in this new context.

The main provisions that are given in UN General Assembly Resolutions No. A/70/174 (2015) and No. A/RES/76/19 (2021), Constitution of Ukraine (1996) and other laws and regulations define key aspects of ensuring and ensuring information sovereignty and information security, but do not always consider new forms of information aggression: cyber-attacks, conceptual influences, and hybrid disinformation campaigns. Hybrid warfare ("sixth generation war") is characterised by the use of classical and non-classical, conventional (weapons) and non-conventional (information influence), military and non-military methods. They are mobile in nature. P. Karber (2015) identified 4 military and 4 non-military factors of hybrid warfare. It refers to the use of traditional military convention forces, special operations forces, non-traditional, non-conventional forces, and proxy forces as 4 military forces. The non-military component is characterised by political and economic factors – cyberspace and the media space. According to Boris Bidichev, this is "propaganda, information wars, and everything related to it. And all these factors are closely intertwined. The most dangerous and surprising thing for the military in this war is that one enemy uses one of the factors, the other responds to completely different ones" (So What is…, 2017). T. Berezyovets (2015) noted that information technologies can ensure the achievement of military goals without the use of conventional weapons, using information resources as means of mass destruction. This provision was confirmed in the facts of mass cyber-attacks on critical infrastructure, manipulative information campaigns aimed at demoralising the population, and attempts to influence international opinion on the legitimacy of the aggressor's actions. In addition, information aggression is increasingly carried out through a complex impact on the emotional and psychological state of society. As noted by V. Polyakova (2022), information attacks are not aimed at the physical destruction of facilities, but at undermining trust, unity and will to resist by disinformation, reducing morale and forming a favourable attitude to the actions of the aggressor among a part of the audience. This approach illustrates the reorientation of the goals of war – from physical to mental control over the space and behaviour of citizens.

Another conceptualisation of hybrid warfare was proposed by D. Vedeneyev (2019), who focused on undermining the moral, political, and informational stability of the enemy. The main goal of this type of war is to weaken the state through non-military, "non-contact" methods of influence, which leads to a decrease in its ability to defend itself, imposing political and socio-cultural models that are beneficial to the external aggressor. This approach helps to understand the role of information law as a tool for protecting sovereignty in a new type of conflict in a new way. Hybrid warfare does not have a frontal offensive line, so there are no legal and moral norms and standards for it, and, above all, as evidenced by the beginning of the Russian-Ukrainian war in 2022, combat operations are conducted without an official declaration of war.

While considering the essence of information warfare, it should be noted that this war, through information attacks, using advanced information technologies, penetrates, first of all, into the daily life of citizens, which is especially important in the context of digitalisation and the impact of artificial intelligence on the security policy of states (Sulowski, 2023). However, the danger of information attacks lies in the fact that if they are successfully implemented, society is undermined from within. There are three goals of information warfare: control of the information space for use for their own purposes; control of information and information flows for conducting information attacks on the enemy; improving the efficiency of the armed forces through military information functions (Denisyuk, 2021).

Summarising the above, it can be argued that information warfare requires a radical rethinking at the level of both legal terminology and national information policy. It goes beyond the classical concepts of "threat" and "defence" – its specificity lies in the combination of tools of influence, including propaganda, cybercrime, manipulative narratives and psychological operations, which do not always fall under the existing legal norms. That is why an important task is to adapt information law to the conditions of such a non-standard form of military conflict. From the above, it can be concluded that the analysis of the problems of conducting a hybrid war by Russia against Ukraine from the standpoint of the science of information law has the following features:

- hybrid warfare involves a wide range of information aspects, from disinformation to cyber threats. The analysis of this conflict allows researchers and practitioners to explore new approaches, norms and tactics in solving problems that arise in the connection with this form of manifestation;
- investigation of the role of hybrid warfare through the prism of the science of information law allows outlining the purposefulness of scientific developments aimed at improving ways to protect personal rights and freedoms of citizens, in particular, in the field of privacy, freedom of speech, and access to objective information;
- with the help of effective mechanisms, scientists of information and other branches of law focus their attention on research related to the improvement of effective tools for legal regulation of relations in the information space, which will qualitatively contribute to the prevention of information attacks and ensuring the optimal development of Information law during hybrid wars;
- analysis of the emergence and localisation of threats of hybrid warfare in the information context is an important argument for improving international scientific cooperation in the field of information law and developing common conceptual theoretical, methodological and practical bases in countering hybrid conflicts.

Analysis of the Law of Ukraine No. 2849-IX (2022) indicates the introduction of a number of novelties aimed at limiting the spread of hostile propaganda, in particular, banning content that justifies armed aggression. However, the legislation still does not have a clear legal definition of disinformation as a separate offence, which complicates law enforcement practice. The EU countries have already established effective legal mechanisms to counter information threats, in particular, disinformation during electoral processes. An example is the Law of France No. 2018-1202 "On Combating the Manipulation of Information" (2018), which provides an opportunity for rapid judicial response to the dissemination of deliberately false information during the election campaign. The law provides, in particular, the obligations of online platforms to disclose sources of funding for political advertising, identify customers of content, mark sponsored information and cooperate with government agencies to stop fake campaigns: the introduction of mechanisms for judicial blocking or refuting fake information in a short time; the obligation of platforms to disclose sponsors of political advertising and label propaganda content; the creation of a centralised information security monitoring body with the authority to detect and neutralise information threats; the expansion of the powers of the national council for television and radio broadcasting and the State Special Communications Service to control the information space during martial law.

According to the Decree of the President of Ukraine No. 447/2021 (2021), cyber-attacks are officially recognised as one of the key tools of hybrid aggression. The document defines the need to harmonise Ukrainian legislation with EU approaches – Directive of the European Parliament and of the Council No. 2022/2555 (2022). In practice, this implementation is slow. During large-scale attacks on government websites and critical infrastructure in 2022-2023, Ukraine actually used administrative methods of response, while the issue of the aggressor's legal responsibility remains unresolved in the international legal plane. The situation is further complicated by the fact that the Law of Ukraine No. 2297-VI (2010) does not comply with the requirements of the GDPR (2016), which creates a regulatory gap in the face of growing cyber threats. During the war, the risk of leakage of personal information from registers, databases of medical and social institutions increases. At the legislative level, the procedure for restricting access to personal data during martial law and the responsibility for their unauthorised use by third parties, in particular by the aggressor, was not detailed. Another discrepancy with EU law is the lack of a mechanism for transparent co-regulation with digital platforms in Ukraine, similar to the EU Code of Practice on Disinformation (2022). This limits the state's ability to respond effectively to real-time information campaigns (Katerynych, 2022). In addition, the tools of legal control over botnets and coordinated information attacks are not systematised.

According to UN General Assembly Resolution No. A/RES/76/19 (2021) states are obliged to refrain from interfering in the internal affairs of other states through ICT. However, Russia systematically violates these norms by using information platforms for conducting psychological operations and information influence. Ukraine can initiate appropriate changes through international forums, based on its own latest legislative experience. The legal basis of the changes was consolidated in the Decree of the President of Ukraine No. 152/2022 "On the Implementation of a Unified Information Policy under Martial Law" (2022). According to Article 64 of the Constitution of Ukraine (1996), during a state of war or emergency, certain rights and freedoms of citizens may be temporarily restricted. The restrictions established by the law consisted in coordinating the activities of the mass media, forming unified information messages. Along with this, Law of Ukraine No. 2849-IX (2022), which came into force under martial law, also included provisions that strengthened control over the information field. These measures helped to quickly neutralise chaotic or hostile

information activity in the first months of a full-scale invasion. The centralisation of information flows made it impossible for independent editorial content to exist, which became the subject of discussion among both journalistic communities and human rights organisations. It should also be noted that journalists, especially those who work in frontline zones or document war crimes, face a number of legal barriers. The activities of military censorship, the requirements for coordination of materials with the General Staff of the Armed Forces of Ukraine and restrictions on access to infrastructure facilities force editorial offices to adapt their work to new realities. All this creates a challenge: how to ensure the effective work of the media without compromising national security is an issue that requires an expanded legal understanding and amendments to the legal regulation of freedom of speech during martial law. The way out of this situation is to adapt the European practice of media self-regulation (for example, in the Scandinavian countries), where even during crises the autonomy of editorial policy remains with clear rules of responsibility (Hurkivska, 2024).

Another key area of restrictions is access to public information. The executive branch has temporarily restricted or completely suspended certain open data tools, including registers of property rights, public procurement, and court decisions. The motive was the need to protect critical information from being used by the enemy. However, the experience of educational projects implemented during the war, such as SEEDUE4UA-101085267, demonstrates how the transformation of information submission forms (through a combination of synchronous and asynchronous formats) becomes a forced but effective tool for adapting to conditions of limited or unstable information access. In such cases, not only the technical approach changes, but also approaches to the development of critical thinking, emotional stability, and the ability to integrate information are revised, which is especially important in a hybrid war.

An analysis of international practice confirms that even in times of armed conflict, states are obliged to comply with the basic standards of freedom of speech and access to information enshrined in the International Covenant on Civil and Political Rights (1966) (Article 19) and the European Convention on Human Rights (1950) (Article 10). Both documents recognise the right to restrict freedom of expression during emergencies, but emphasise that such restrictions must be necessary, proportionate and legal. The practice of the European Court of Human Rights (ECHR, the Court) also sets limits on permissible state interference in freedom of speech. In the case of Şener v. Turkey (2000), the Court stressed that even in a situation of threat to national security, any restriction should be based on a clear legal basis and not turn into a mechanism of general censorship. The Court expressed a similar position in cases related to the conflicts in Chechnya and Kosovo, where it recognised the right of participating states to restrict media freedom only in exceptional, specifically justified cases.

Also important is the practice of the United States, which, in the context of a hybrid or permanent military threat, uses a model of conditional regulation: the state provides basic freedom of expression, but within the framework of codes of responsibility for the dissemination of fake narratives, coordination with platforms, and the distinction between journalistic activities and information sabotage (USA Patriot Act, 2001). For Ukraine, such a model may be relevant in the medium term. It provides for a combination of legislative control, independent regulation, and self-regulation of the media. In practice, this can be implemented based on such cases as the Roth v. United States (1957), where the judiciary stated that "the unconditional wording of the First Amendment was not intended to protect every expression", and the case FCC v. Pacifica Foundation (1978), where it was stated that "the content of broadcasting a radio station... has no right to absolute constitutional protection". Those cases had shown that freedom of expression and freedom of information were not absolute and could be restricted. The transition from rigid centralisation of the information space to a flexible system of correlation between the media, the state and civil society would meet European standards and simultaneously preserve national interests in war context.

As for the Law of Ukraine No. 2297-VI "On Protection of Personal Data" (2010), the changes made to it in recent years mainly focus on adapting to EU standards, in particular, based on GDPR (2016). However, there are a number of problems with the actual implementation of these changes in practice, in particular, in the context of working with sensitive data in the context of constant cyber threats and military conflict. The introduction of new security standards for the processing of personal data in war conditions is critical, because personal data can become a target for cyber-attacks or be used for manipulations that undermine citizens' trust in state institutions. Considering the previous comments, it is worth implementing such restrictions within the framework of soft paternalism, the application of which in the field of data protection was disclosed by I. Patricheev (2025). In general, this requires a more detailed and in-depth analysis, since their effectiveness in protecting the information rights and security of citizens has not yet been fully evaluated, in particular, in the context of hybrid threats. As of 2025, there is no consensus in the national legal opinion of science on what information should be considered sensitive, which ultimately affects the sustainable information space and, above all, information security. Therefore, further adaptation of Ukrainian legislation to the realities of global information warfare and innovations in cybersecurity is necessary to ensure the proper level of legal protection of citizens.

Given this aspect, it is advisable to develop specialised legislative initiatives to process particularly sensitive information in war context, which will help ensure a high level of cybersecurity without violating the rights of citizens. It is necessary to introduce new legal instruments that will effectively counteract hybrid threats, in particular, through the modernisation of existing laws and regulations and the adoption of new laws that consider advanced information security challenges. Simultaneously, it is important to ensure a balance between the protection of national security and human rights, which will become the basis for the stable development of information law in war context. In the search for a concept to substantiate recommendations for improving information law in the context of the Russian-Ukrainian war, their development requires a comprehensive approach and consideration of current challenges facing modern society. The key areas for further development of information law are the following:

1. Creation of effective legislative mechanisms to ensure the implementation of innovation processes: the

development of Information law, considering fleeting information and communication technological changes, should be aimed at creating flexible innovation legislation adapted to qualitatively new scientific achievements, such as artificial intelligence, blockchain, and other technological innovations.

2. Ensuring cybersecurity: the development of information legislation in the field of cybersecurity protection should be focused on defining clear standards and requirements for detecting and countering cyber threats, and providing practical assistance in eliminating the consequences of cyber incidents.

3. Protection of intellectual property rights: recording of violations of intellectual property rights should be carried out through the active use of electronic technologies and the application of digital security measures. Strengthening the protection of intellectual property rights as an integral part of gross domestic product in the digital environment, through effective copyright, patent, and trademark mechanisms, can be a reliable lever to increase productivity and reduce costs in industry.

4. Development of information access policy: ensuring transparency and access to information based on contemporary information and policy doctrine is to develop a flexible state policy that, under martial law, while ensuring confidentiality and protection of personal data, will promote reliable access to information.

5. International cooperation: plays an important role in conceptual development and optimisation of information law in the context of Russian aggression. Active participation in international forums and agreements aimed at solving global problems of legal support of information security.

6. Protection of personal data: the effectiveness of protection of personal data of citizens as a critical aspect of information law should be ensured through the development and improvement of mechanisms for controlling the collection, storage, and processing of personal information.

7. Ensuring information security in the field of national defence: the development of special norms and state policies in ensuring information security in the field of national defence includes effective protection against cyber-attacks, the use of information weapons, and other tools.

The analysis of regulatory processes that accompany the transformation of information law in Ukraine under martial law indicates the need to develop a comprehensive, balanced model of information security that considers both national challenges and international standards. Based on the practice of implementing emergency information regimes, in particular, media coordination, restricting access to public information, and actively responding to external information attacks, there is a shift in emphasis from the liberal model of freedom of speech to the conditionally restrictive one designed to counter hybrid threats. However, comparison with foreign practice (France, USA, ECHR) allows outlining the potential for the development of a flexible legal mechanism that combines elements of self-regulation, state control, and international cooperation. Maintaining the proportionality of restrictions, transparency of legal regulation, and ensuring effective legal protection of citizens in the digital age is crucial for this approach. In the long run, this should be reflected in updated legislative initiatives aimed at adapting to new forms of disinformation, cyber threats and sensitivity to human rights, which will allow building a sustainable information infrastructure even in the context of war.

Conclusions

The study highlighted the transformation processes in the field of information law of Ukraine under martial law and hybrid information law. In order to assess the effectiveness of already implemented changes in legislation and substantiation of legal mechanisms that can ensure the proper level of information security in the new conditions, the legal nature of hybrid warfare, features of information aggression were analysed and the main threats associated with disinformation, cyber-attacks and manipulations in the digital environment were identified. The study described the regulatory framework of Ukraine in the field of information security, in particular, under martial law, and analysed its compliance with international standards.

The results of the study revealed such key aspects as the need for normative specification of the concept of disinformation, the introduction of effective mechanisms for countering information attacks, and the harmonisation of Ukrainian legislation with EU law (in particular, in the context of GDPR, NIS2, Code of Practice on Disinformation). The paper also analysed the experience of France, the United States, and the ECHR in balancing freedom of speech and security in crisis context. It was revealed that the administrative model of response prevails in Ukraine, but the tools of self-regulation and co-regulation remain undeveloped. In this regard, the importance of adapting the Ukrainian information policy to the context of long-term hybrid confrontation was emphasised, in particular, through the regulatory details of processing sensitive information, including personal data.

The results obtained indicated that the modern information law of Ukraine was at the stage of dynamic development, but required significant modernisation in both conceptual and instrumental dimensions. The analysis showed that effective legal response to information aggression involved a combination of three levels: strategic (national policy), regulatory (laws and bylaws), and operational (mechanisms for monitoring, responsibility, coordination with digital platforms). All of the above suggests that information law in war context is not only a tool of protection, but also a factor of national stability, which determines the ability of the state to counteract external information pressure while maintaining democratic principles.

Summarising the results obtained, it can be noted that further research should be directed to the development of concepts of co-regulation in the field of media and digital platforms, the investigation of mechanisms for protecting the rights of journalists in front-line context, and to the development of legal approaches to the qualification of information wars in international law.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of interest

None.

References

[1] Berezyovets, T. (2015). *Annexation: The Crimean Peninsula. Chronicles of "Hybrid War"*. Kyiv: Bright Books.
[2] Brantly, A. (2022). Battling the bear: Ukraine's approach to national cyber and information security. In M.D. Cavelty & A. Wenger (Eds.), *Cyber security politics: Socio-technological transformations and political fragmentation* (pp. 157-171). New York: Routledge doi: 10.4324/9781003110224-13.
[3] Chmyr, Y., Deineha, M., Shchepanskiy, E., Koshelenko, A., & Kozenko, R. (2023). Tools for counteracting information aggression use of elements of information war in Ukraine. In O. Radchenko, V. Kovach, I. Semenets-Orlova & A. Zaporozhets (Eds.), *National security drivers of Ukraine. Contributions to political science* (pp. 258-299). Cham: Springer. doi: 10.1007/978-3-031-33724-6_17.
[4] Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.
[5] Decree of the President of Ukraine No. 152/2022 "On the Unified Information Policy in Wartime". (2022, March). Retrieved from https://zakon.rada.gov.ua/laws/show/152/2022#Text.
[6] Decree of the President of Ukraine No. 447/2021 "On the Cybersecurity Strategy". (2021, August). Retrieved from https://zakon.rada.gov.ua/laws/show/447/2021#Text.
[7] Denisyuk, Zh.Z. (2021). Propaganda and counter-propaganda in the context of state information policy strategies. *Mechanisms of Public Administration*, 32(2), 46-51. doi: 10.32838/TNU-2663-6468/2021.2/08.
[8] Directive of the European Parliament and of the Council No. 2022/2555 "On Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive)". (2022, December). Retrieved from https://surl.lt/slicwu.
[9] European Convention on Human Rights. (1950, November). Retrieved from https://zakon.rada.gov.ua/laws/show/995_004.
[10] Fedoniuk, S., Karpchuk, N.A., & Yuskiv, B. (2023). Ukraine's information security policy: At the crossroads between Russia and the West. *Czech Journal of Political Science*, 30(3), 184-205. doi: 10.5817/PC2023-3-184.
[11] Hurkivska, A. (2024). Ukraine's information security resilience amidst contemporary warfare: Policy context in development. *SSRN*. doi: 10.2139/ssrn.4896495.
[12] Hurzhi, T. (2018). Information law: Challenges of hybrid warfare. *Public Law*, 4, 16-26.
[13] Judgment of the European Court of Human Rights in Case No. 26680/95 "Şener v. Turkey". (2000, July). Retrieved from https://hudoc.echr.coe.int/eng?i=001-58753.
[14] Judgment of the Supreme Court of the United States in Case "Roth v. United States". (1957, October). Retrieved from https://www.loc.gov/item/usrep354476/.
[15] Judgment of the Supreme Court of the United States in Case No. 77-528 "FCC v. Pacifica Foundation". (1978, October). Retrieved from https://www.law.cornell.edu/supremecourt/text/438/726.
[16] Karber, P.A. (2015). *Russia's new generation warfare*. Retrieved from https://www.ausa.org/articles/russia%E2%80%99s-new-generation-warfare.
[17] Katerynych, P. (2022). Comparative analysis of the information security environment in Ukraine and Poland (survey of journalists and editors). *Communication and Society*, 35(4), 37-53. doi: 10.15581/003.35.4.37-53.
[18] Khriapynskyi, A., Khmyrov, I., Svoboda, I., Shevchuk, M., & Iastrebova, V. (2024). State information security strategies in conditions of hybrid threats. *Amazonia Investiga*, 12(69), 84-93. doi: 10.34069/AI/2023.69.09.7.
[19] Kormych, L., Krasnopolska, T., & Zavhorodnia, Y. (2024). Digital transformation and national security ensuring. *European Political and Law Discourse*, 11(1), 29-37. doi: 10.46340/eppd.2024.11.1.4.
[20] Law of France No. 2018-1202 "On Combating the Manipulation of Information". (2018, December). Retrieved from https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559?utm.
[21] Law of Ukraine No. 2297-VI "On Protection of Personal Data". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text.
[22] Law of Ukraine No. 2657-XII "On Information". (1992, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2657-12#Text.
[23] Law of Ukraine No. 2849-IX "On Media". (2022, December). Retrieved from https://zakon.rada.gov.ua/laws/show/2849-20#Text.
[24] Lysenko, S., Marukhovskyi, O., Krap, A., Illiuschenko, S., & Pochapska, O. (2023). The analysis of world information warfare and information security in the context of the Russian-Ukrainian war. *Studies in Media and Communication*, 11(7), 150-158. doi: 10.11114/smc.v11i7.6414.
[25] Nuritdinov, N. (2024). Socio-cultural factors of the effective use of critical thinking in the development of modern legal knowledge. *Pubmedia Social Sciences and Humanities*, 2(2). doi: 10.47134/pssh.v2i2.294.
[26] Patricheev, I. (2025). Legal paternalism's influence on the balancing data protection and fundamental rights. *Law Journal of the National Academy of Internal Affairs*, 15(1), 48-58. doi: 10.63341/naia-chasopis/1.2025.48.
[27] Polyakova, V. (2022). *Information warfare: What is it and why it is important to understand its nature*. Retrieved from https://gwaramedia.com/informaczijna-vijna-istorichni-prikladi-najnebezpechnishoi-zbroi/.
[28] Pravdiuk, A. (2022). The state and current issues of legal regulation of cyber security in Ukraine. *European Political and law Discourse*, 9(3), 19-28. doi: 10.46340/eppd.2022.9.3.3.
[29] Pravdiuk, A. (2023). Information security of Ukraine: information influence and information wars. *European Political and law Discourse*, 10(1), 111-121. doi: 10.46340/eppd.2023.10.1.6.
[30] Regulation of the European Parliament and of the Council No. 2016/679 "On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)". (2016, April). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[31] Saeed, S., Altamimi, S.A., Alkayyal, N.A., Alshehri, E., & Alabbad, D.A. (2023). Digital transformation and cybersecurity challenges for business resilience: Issues and recommendations. *Sensors*, 23(15), article number 6666. doi: 10.3390/s23156666.
[32] So What is Hybrid Warfare? And Is Hybrid Warfare Present in Ukraine? (2017). Retrieved from https://www.armyfm.com.ua/tak-shho-zh-take-g%D1%96bridna-v%D1%96jna-%D1%96-chi-g%D1%96bridna-v%D1%96jna-v-ukra%D1%97n%D1%96/.
[33] Sopilko, I., Svintsytskyi, A., Krasovska, Y., Padalka, A., & Lyseiuk, A. (2022). Information wars as a threat to the information security of Ukraine. *Conflict Resolution Quarterly*, 39(3), 333-347. doi: 10.1002/crq.21331.
[34] Sulowski, S. (2023). *Security challenges at the dawn of a new international order*. Berlin, Bern, Bruxelles, New York, Oxford, Warszawa, Wien: Peter Leng.
[35] UN General Assembly Resolution No. 48/15 "Return or Restitution of Cultural Property to Their Countries of Origin". (1993, November). Retrieved from https://zakon.rada.gov.ua/laws/show/995_718#Text.
[36] UN General Assembly Resolution No. A/70/174. (2015, June). Retrieved from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement.
[37] UN General Assembly Resolution No. A/RES/76/19. (2021, December). Retrieved from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/377/51/PDF/N2137751.pdf?OpenElement.
[38] Vedeneyev, D. (2019). *From Machiavelli to robot wars: The grammar of "hybrid" warfare*. Retrieved from https://old.defence-ua.com/index.php/statti/publikatsiji-partneriv/7236-vid-makiavelli-do-viyn-robotiv-hramatyka-hibrydnoyi-viyny-2.
[39] Zadorozhny, H. (2021). Consistent war – the leading form of geoeconomic subjugation of consciousness as a new object of labor in the context of neoliberal globalization. *Bulletin of Economic Science of Ukraine*, 1(40), 199-206. doi: 10.37405/1729-7206.2021.1(40).199-206.

Інформаційне право в умовах інформаційної агресії

Леонтій Чистоклетов
Доктор юридичних наук, професор
Національний університет «Львівська політехніка»
79005, вул. Князя Романа, 1/3, м. Львів, Україна
https://orcid.org/0000-0002-3306-1593
Юрій Назар
Доктор юридичних наук, професор
Львівський державний університет внутрішніх справ
79007, вул. Городоцька, 26, м. Львів, Україна
https://orcid.org/0000-0002-8059-4413
Олександра Хитра
Доктор юридичних наук, професор
Львівський державний університет внутрішніх справ
79007, вул. Городоцька, 26, м. Львів, Україна
https://orcid.org/0000-0002-3632-5101
Дмитро Забзалюк
Доктор юридичних наук, професор
Львівський державний університет внутрішніх справ
79007, вул. Городоцька, 26, м. Львів, Україна
https://orcid.org/0000-0002-1041-0148
Юлія Комісарчук
Кандидат юридичних наук, доцент
Львівський державний університет внутрішніх справ
79007, вул. Городоцька, 26, м. Львів, Україна
https://orcid.org/0000-0002-5079-334X

Анотація. Проблематика інформаційного права в умовах гібридної війни, що включає питання кібербезпеки, протидії дезінформації, захисту інформаційного суверенітету та свободи слова, набула особливої актуальності та стала однією з ключових сфер юридичних досліджень у відповідь на широкомасштабну інформаційну агресію проти України. Метою роботи було вивчення реакції регулятора на зовнішні у вигляді гібридної інформаційної війни. У дослідженні застосовано методи порівняльного аналізу, системного підходу, формально-логічного методу. У ході дослідження було проаналізовано ключові аспекти функціонування інформаційного права в умовах воєнного стану, зокрема його спроможність забезпечити свободу слова та доступ до достовірної інформації. Було досліджено правові механізми, які забезпечують інформаційну безпеку, з урахуванням новітніх форм інформаційної агресії, включно з кіберзагрозами, пропагандою, дезінформацією та маніпуляцією у соціальних мережах. Було узагальнено практику міжнародного співробітництва у сфері інформаційної безпеки та встановлено, що ефективна протидія гібридній війні потребує адаптації правового середовища до умов новітніх інформаційно-комунікаційних технологій. Проаналізовано сучасні законодавчі ініціативи в Україні у сфері інформаційної безпеки та запропоновано шляхи вдосконалення національного інформаційного законодавства, зокрема у напрямах кібербезпеки, захисту персональних даних, протидії фейкам і регулювання діяльності медіа. Практична цінність роботи полягає у можливості використання її результатів законодавцями, правозастосовними органами, науковцями та фахівцями в галузі кібербезпеки для розробки та впровадження ефективної інформаційної політики в умовах воєнного конфлікту

Ключові слова: інформаційна безпека; цифрове середовище; кіберзагрози; свобода вираження; правове регулювання; інформаційні маніпуляції