NUOVA ANTOLOGIA MILITARE
RIVISTA INTERDISCIPLINARE DELLA SOCIETÀ ITALIANA DI STORIA MILITARE

NAM Studies & Documents

Special Dossier October 2025
Ukraine Military and Wartime Law

Edited by Ganna Sobko

Società Italiana di Storia Militare

Nuova Antologia Militare

Rivista interdisciplinare della Società Italiana di Storia Militare

Periodico telematico open-access annuale (www.nam-sism.org)

Registrazione del Tribunale Ordinario di Roma n. 06 del 30 Gennaio 2020

Scopus List of Accepted Titles October 2022 (No. 597)

Rivista scientifica ANVUR (5/9/2023) Area 11, Area 10 (21/12/2024)

Direzione, Via Bosco degli Arvali 24, 00148 Roma

Contatti: direzione@nam-sigm.org ; virgilio.ilari@gmail.com

Grafica: Nadir Media Srl - Via Giuseppe Veronese, 22 - 00146 Roma

info@nadirmedia.it

Gruppo Editoriale Tab Srl -Viale Manzoni 24/c - 00185 Roma

www.tabedizioni.it

ISSN: 2704-9795

ISBN Fascicolo 979-12-5669-221-7

NUOVA ANTOLOGIA MILITARE
RIVISTA INTERDISCIPLINARE DELLA SOCIETÀ ITALIANA DI STORIA MILITARE

NAM Studies & Documents

Special Dossier October 2025
Ukraine Military and Wartime Law

Edited by Ganna Sobko

Società Italiana di Storia Militare

Monument to Yaroslav The Wise, Grand Prince of Kyiv (978-1054)
In the Yaroslav Mudryi National Law University,
61024, 77, Hryhorii Skovorody Street, Kharkiv, Ukraine
Photo Tala Tamila (2015) CC SA 4.0 (Wikimedia Commons)

Information sovereignty of the state in the context of hybrid threats in the digital age: Legal protection mechanisms in Ukraine

by Oleksandr Tykhomyrov[1], Denys Tykhomyrov[2], Liudmyla Radovetska[3], Ihor Bohdan[4]

Abstract. The growing proportion, variety and technical level of cyberattacks in the spectrum of hybrid threats aimed at Ukraine's information resources makes the issue of information sovereignty relevant. From disinformation campaigns to direct cyberattacks on critical information infrastructure, such attacks pose a direct threat to the security of the state, its stable operation and functioning in times of the digital age, further development of information technology and the corresponding formation of new forms, dimensions, and principles of the information society. Legal mechanisms for protecting Ukraine's information space need to be strengthened and adapted to new challenges. This is the reason for the relevance of the scientific research. The purpose of the research is to analyse the legal aspects of protection of information systems of Ukraine, key aspects of information sovereignty and to assess their effectiveness in the context of the hybrid threats realization in modern conditions. To achieve the research goal, it can be used the following research methods: general philosophical method, descriptive method, method of system analysis, synthesis, dialectical method, methods of deduction and induction. Eliminating gaps and inconsistencies in existing legislation and adapting to the best international practices, the conclusions of the research provide a new perspective on Ukraine's information security, information sovereignty and

1 Department of Information Security of the State, National Academy of the Security Service of Ukraine, 03022, 22 Maksymovych Str., Kyiv, Ukraine. https://orcid.org/0000-0001-5163-6584.

2 Department of Theories, Histories and Philosophies of Law, National Academy of Internal Affairs, 03035, 1 Solomianska Sq., Kyiv, Ukraine. https://orcid.org/0000-0001-8366-8564.

3 Department of Theory and History of State and Law, National Academy of the Security Service of Ukraine, 03022, 22 Maksymovych Str., Kyiv, Ukraine. https://orcid.org/0000-0001-9013-8246.

4 Department of Theories, Histories and Philosophies of Law, National Academy of Internal Affairs, 03035, 1 Solomianska Sq., Kyiv, Ukraine. https://orcid.org/0009-0001-3880-8967.

NAM, Anno 6 – Special Dossier
DOI: 10.36158/97912566922178
Ottobre 2025

protection against hybrid threats. In turn, proposals were also made to develop the concept of a national strategy for information sovereignty, including the improvement of legal norms and integration with international standards, which together contributed to the achievement of the goal.

Keywords: cybersecurity; digitalization; hybrid threats; information law; information security; information sovereignty; state defense.

1 Introduction

The information society, due to its development and formation, creates significantly new conditions and frameworks for the existence of the state, its interaction with other participants in information relations (states and international organisations, as well as domestic actors). That is why ensuring information sovereignty directly depends on the interconnection with all spheres of society and is carried out both within the state and outside it – that is, in the global information space and in the purely national one in the course of ensuring and implementing the functions of the state and the direct presence of an information component in such functions (Chander & Haochen, 2023).

The twenty-first century has created conditions in which technological progress and the information space have become a new battlefield and a component of state security and defence. This is evidenced by the massive cyberattacks on Ukraine's critical information systems after the start of the full-scale invasion, which were aimed at creating hybrid threats and losing confidence in the state as such. Therefore, it can confidently be said that there is a threat to the sovereignty of the state. Such threats include the use of traditional and non-traditional models of information influence, which weakens the state's defence, while making the protection of national information sovereignty an urgent priority. Being the cornerstone of national security, the protection of this sovereignty is not just a technical problem, but a legal and strategic imperative that requires reliable mechanisms to counteract growing risks (Khmyrov, 2023).

The acceptable state of information sovereignty security should be noted that it includes not only an active aspect, but also the creation of conditions that will facilitate the implementation of all measures to protect it. After all, if Ukraine's sovereignty is generally ensured not only by the formal legal entrenchment of this category in the Constitution and the guarantee of sovereignty through military,

economic, diplomatic and other means, but also emphasised by the very fact of the existence and activities of the government, police, banking system, development of legislation and clearly established borders, has a strong economic component, etc. (Kotsur et al., 2023).

Information sovereignty is defined as the ability and right of the state to independently formulate and implement its information policy, to dispose of information resources, available infrastructure and ensure security in the information space at its own discretion; as well as to have the ability to protect the population from the results of mass cyberattacks by an external enemy, resistance to information warfare, which is based on the ability of the state to manage the information received by the population, which requires the creation of appropriate conditions.

Cyber threats are an obvious fact that their direct consequence is to cause damage to the state, society and individuals in the information sphere. These threats are expressed in four different spheres of influence: the impact on society, i.e. psychological and informational threats; the impact on digital infrastructure, namely technological threats; the legal sphere, which directly regulates relations in the information environment and where legal threats arise; and political threats, which are manifested in institutional imperfections, censorship, etc. (Pravdyuk, 2024).

In the context of Russia's full-scale invasion of Ukraine, the main threats to Ukraine's security and defence are those directly related to the aggression of Russia and its controlled entities. Such threats are manifested by the aggressor's communication and information advantages in the temporarily occupied territories; Russia's active conduct of certain information operations; the insufficient development of the national information infrastructure, which negatively affects Ukraine's ability to counter this level of information threats and act within the framework of Ukraine's national interests; gaps in legislation on the regulation of information relations; and uncertainty in strategic communications (Solodka, 2024).

It is believed that the relevance of this study is directly related to the growing number of hybrid threats that are directly aimed at undermining Ukraine's security. Starting from disinformation campaigns to direct cyberattacks on critical information infrastructure, such direct attacks pose a direct threat to the security of the state, its stable operation and functioning in times of technological progress and development of information systems. That is why ensuring information

sovereignty is such an important aspect of preserving Ukraine's independence. This article aims to examine these issues and the need to ensure information sovereignty, to explore the legislative framework developed to protect the country's information space and to suggest ways to strengthen it.

If the importance of the findings of the study is considered, it is ensured by the contribution to a much broader discourse on Ukraine's information sovereignty and hybrid warfare as such. While existing studies have explored the technical aspects of cyberattacks or the geopolitical implications of hybrid threats, few have comprehensively delved into the legal mechanisms underpinning the state's response. This research article builds on previous studies by directly analysing the adaptation of Ukrainian legislation with a forward-looking strategy, distinguishing it from more generalised approaches that do not take into account the nuances of the national context. Moreover, this article aims to fill the existing gaps in the information relations framework, while offering a balance between the analysis of legal theory, international harmonisation and, accordingly, direct implementation. Taken together, this once again underlines the relevance of the study.

In terms of scientific novelty, it can confidently be pointed out that the proposals for a national strategy of information sovereignty take into account the unique geopolitical context of Ukraine. By eliminating gaps and inconsistencies in existing legislation and adapting to the best international practices, the conclusions of the research paper provide a new perspective on Ukraine's information security and protection against hybrid threats. It is also important to note that this article emphasises the intersection of information law and national security, providing a context-specific lens that is practical and innovative (Neustroiev, 2021).

That is why the purpose of this research is to analyse the legal aspects of protection of information systems of Ukraine, key aspects of information sovereignty and to assess their effectiveness in the context of hybrid threats. The objectives of the research article are: to study the legal aspects of protection of critical information systems; to determine the peculiarities of harmonisation of Ukrainian legislation with international cybersecurity standards; to understand the role of information law in ensuring national security in the digital age; to provide proposals for the concept of a national strategy of information sovereignty of an integrative nature that takes into account the improvement of legal norms and integration with international standards (Sopilko, 2024).

2. Materials and Methods

Taking into account the relevance of the study, the purpose, and the outlined tasks, the following methods of scientific knowledge were used: general philosophical method, descriptive method, method of system analysis, synthesis, dialectical method, and methods of deduction and induction. All scientifically significant conclusions were obtained through the active use of the above methods, both individually and in combination. Each stage of the research was accompanied by the use of the general philosophical method. It helped us to formulate the main conclusions of the research, which in turn contain a new view of Ukraine's information security, information sovereignty and protection against hybrid threats.

The descriptive method was an important method of cognition in the research, which helped to provide a detailed description of the legal aspects of protecting critical information systems, and also helped to identify vulnerabilities in the legal mechanisms of Ukraine in terms of information relations. Using this method and combining its application with another method – the method of systematic analysis – It reviewed the current legislation of Ukraine related to information security and protection against hybrid threats, which further contributed to a comprehensive study.

The systematic analysis method was also used to review international information security standards, which may have a positive impact on Ukraine's efforts to improve its legislation. The synthesis method was used, which in combination contributed to understanding the current state of Ukrainian legislation and identifying areas that need to be improved. With the help of the dialectical method, the synthesis method, and the general philosophical method, it was possible to understand the benefits of harmonizing Ukrainian legislation with international standards, which manifests itself in the areas of enhanced defense, cooperation with allies, and increased resilience to hybrid threats. The dialectical method also contributed to a better understanding of the concept of information sovereignty, hybrid threats in general, and those hybrid threats that pose a heightened risk to Ukraine as part of Russia's aggression.

Using the deductive method, the strategic role of information law in ensuring national security and defense in the digital age was formed. Using the inductive method, deductive method, and system analysis method, the research develops strategic recommendations for strengthening Ukraine's information sovereignty

through legal mechanisms as an integral component of Ukraine's national security, taking into account the unique geopolitical context of Ukraine. Reasonable and balanced use of all the above methods contributed to the achievement of the research goal and objectives, while the conclusions of the research work contain a new perspective on Ukraine's information security, information sovereignty and protection against hybrid threats.

3. Results and Discussion

2.1. *Legal aspects of critical information systems protection*

Against the backdrop of an active hybrid war and frequent threats, Ukraine is obliged to improve and develop a legislative framework that will help to actively counter threats. As of today, work on legislative documents is actively underway, but it will take both time and resources to cover the entire spectrum of information relations and regulate them accordingly, taking into account martial law. As the importance of cybersecurity continues to grow and legislative responses intensify, a certain imbalance can be observed between the legal regulation of information security and cybersecurity – both in their normative interpretation and in the alignment of strategic goals for their implementation. However, it can be noted that the basis of the legislative framework for cybersecurity is the Constitution of Ukraine (Verkhovna Rada of Ukraine, 1996). The Constitution of Ukraine (1996) contains provisions on the protection of personal data, information and citizens' rights that directly relate to the information space.

The legislative framework is also formed by laws and bylaws, to which it must first of all refer the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity in Ukraine." (Verkhovna Rada of Ukraine, 2017). Its provisions define the legal and organisational framework for protecting the vital interests of a person and citizen, society and the state, as well as Ukraine's national interests in cyberspace. The law also sets out the primary goals, principles and directions of Ukraine's cybersecurity policy, defines the range of authorised bodies, reveals the range of their powers and responsibilities, and specifies the basis for coordination between these bodies and other enterprises, institutions and organisations, and citizens in the field of cybersecurity in Ukraine (Verkhovna Rada of Ukraine, 2017).

The basis of liability for unlawful acts in the field of cybersecurity is also set out in the Criminal Code of Ukraine (Verkhovna Rada of Ukraine, 2001). In gen-

eral, criminal liability is incurred for unauthorised interference with the operation of electronic computers, automated systems, computer networks or telecommunication networks; development for the purpose of using, distributing or selling malicious software or hardware, as well as their distribution or sale; unauthorised sale or distribution of restricted information stored in electronic computers, automated systems, computer networks or on media containing such information.

Another important legislative document is the Law of Ukraine "On Information" (Verkhovna Rada of Ukraine, 1992). The provisions of the law are intended to regulate the main aspects of information security, legal relations on information processing, as well as the protection of information as such. At the same time, the Law of Ukraine "On Information Protection in Information and Telecommunication Systems" contains direct requirements for technical protection of information in information systems and imposes a direct obligation on critical infrastructure operators to actively implement cybersecurity systems (Verkhovna Rada of Ukraine, 1994).

It is also worth mentioning the Law of Ukraine "On the State Service for Special Communications and Information Protection of Ukraine", which contains the legal framework for the organisation and operation of the State Service for Special Communications and Information Protection of Ukraine in accordance with the Constitution of Ukraine (Verkhovna Rada of Ukraine, 2006). In 2021, the National Security and Defence Council of Ukraine adopted a decision "On the Cybersecurity Strategy of Ukraine", which was directly aimed at improving the security situation and the overall resilience of the information critical infrastructure. It addressed the issue of protecting both public and private information systems. This Strategy contained information on new challenges and cyber threats and emphasised the role of cybersecurity as a priority in the national security system of Ukraine (Verkhovna Rada of Ukraine, 2021).

The Action Plan for the Implementation of the Cybersecurity Strategy of Ukraine for 2023-2024 was formed, with the main focus on the creation of cyber troops within the Ministry of Defence, providing them with adequate financial, human and technical support to deter armed aggression in cyberspace "and repel the aggressor" (Verkhovna Rada of Ukraine, 2023a). It should also be added that in 2023, the Cabinet of Ministers of Ukraine adopted the Resolution "Some issues of response of cybersecurity entities to various types of events in cyberspace", which is also valuable in the context of cybersecurity (Verkhovna Rada

of Ukraine, 2023a).

In this regard, it should be noted that the Convention on Cybercrime, which was ratified by Ukraine in 2005, plays an equally important role, but with some important reservations. They generally included criminalisation in national legislation of the development or use of software or hardware for unauthorised access, interception of data or interference with data or systems (Verkhovna Rada of Ukraine, 2005). The Law of Ukraine "On critical infrastructure" is worth mentioning when analyzing the issue of cyber defense of critical infrastructure (Verkhovna Rada of Ukraine, 2023c), which defines the legal and organisational framework for the creation and smooth operation of the national system of critical infrastructure protection, and the CMU Resolution "On Approval of General Requirements for Cybersecurity of Critical Infrastructure Facilities" (Verkhovna Rada of Ukraine, 2019).

Analysing the peculiarities of these legal acts, it should be noted that since they were adopted at different times, there may often be inconsistencies in terminology, overlapping accountability, gaps and contradictory aspects, lack of provisions for conducting information security audits of critical infrastructure, etc. Moreover, there are problems in the distribution of powers. Therefore, it is quite obvious that the legislative framework needs to be comprehensively revised, coordinated with each other and take into account current trends and the situation in Ukraine. It is also important to note that the effective implementation of the Convention on Cybercrime requires government agencies to take measures to provide more precise and comprehensive definitions of the concept of cybersecurity (Didkivska & Shevchenko, 2024).

The challenges faced during cyberattacks and what needs to be considered when bringing the legal framework into compliance are important. These problems may include low or insufficient cybersecurity skills of personnel, which prevents them from recognizing and responding to threats in a timely manner. This issue should be addressed to ensure continuous education and training in the future (Khudoliy et al., 2024). Another challenge is sophisticated cyberattacks, as attackers usually choose advanced methods that include extensive training, sophisticated tools, and disguise as legitimate activities.

In this case, attention should be focused on creating a mechanism to ensure information systems are capable of responding to this level of threat sophistication (Vasylkivska & Bondarenko, 2023). There is also a need for effective monitoring

tools, including outdated software that will not be relevant to modern cyberattacks. Another issue is the lack of modern artificial intelligence-based solutions for automated anomaly detection (Savchuk, 2024). The lack of rapid adaptation to changing threats is another problem that affects both the regulatory framework and the updating of security systems and signature databases.

The latter aspect can be addressed in the process of allocating financial resources, while the former takes time. Besides, the lack of financial resources is manifested in outdated software and a shortage of qualified personnel with low salaries. Communication between the relevant departments is also problematic, as IT and security departments often work in isolation, which slows down the exchange of information. That is why efforts should be directed at creating unified security protocols and standardizing processes to respond to potential threats in a timely manner (Vorotynskyy, 2024). These problematic aspects and challenges once again emphasise the importance of bringing the regulatory framework in line with the current state of affairs and creating a comprehensive approach to countering cyber threats.

3.2 Harmonisation of Ukrainian legislation with international cybersecurity standards

As part of the scientific study and taking into account the above-analysed legal aspects of critical information systems protection, it is also worth investigating the issue of harmonisation of Ukrainian legislation with international cybersecurity standards within the framework of the EU and NATO activities. It is worth noting that an important vector of the European Union's activities is to ensure cybersecurity and timely response to hybrid threats. The EU's approach is based on several key legal documents, such as the NIS Directive, NIS 2 Directive 2022/2555 and The European Cyber Resilience Act (CRA) (Cyber Risk GmbH, 2024).

In turn, The European Cyber Resilience Act (2024) addresses two key issues, namely: the relatively low level of security of products with digital elements, characterised by the presence of vulnerabilities and inconsistent and untimely updates of security systems to eliminate such vulnerabilities; insufficient understanding and access to information by users, which prevents them from choosing products with appropriate cybersecurity features or using them in a safe manner (H-X Technologies, 2024). In general, the European approach is manifested in a

harmonised and holistic approach to cybersecurity and cyber incident response. For the latter, the EU relies on a network of CSIRTs (Computer Security Incident Response Teams) that coordinate national response teams. Under such conditions, there is a rapid exchange of data on potential and real threats, which creates the appropriate conditions for an effective response to cyber incidents.

As for NATO's activities, it is worth noting that actions aimed at ensuring cyber defence are a priority task in deterrence and defence. It is clear that NATO's focus is on protecting its own information systems, secure activities in the digital space and direct assistance to NATO members in these areas. In 2016, NATO's defence mandate was approved and cyberspace was recognised as a direct area of operations. In the same year, NATO Allies committed to potential cyber defence, and in 2023, this pledge was reinforced by setting new goals to strengthen cyber defence as a priority. This also includes the protection of critical infrastructure (North Atlantic Treaty Organization, 2024).

It is also important to add that at the NATO Summit in Vilnius in 2023, Allies endorsed a new concept to strengthen the contribution of cyber defence to NATO's overall deterrence and defence posture, and launched NATO's Virtual Cyber Incident Support Capability (VCISC) to support national mitigation efforts in response to significant malicious cyber activity. In 2024, the establishment of a NATO Integrated Cyber Defence Centre was raised to promote better awareness of cyber threats, to directly protect networks, and to establish cyberspace as an operational domain (North Atlantic Treaty Organization, 2024).

NATO and the EU cooperate in the area of cyber defence, and therefore such cooperation is indicative for Ukraine in terms of harmonising its legislation with international standards. Moreover, Ukraine's partners will take into account Ukraine's experience in protecting information systems and responding to hybrid threats, while emphasising Ukraine's significant efforts in this area. It is important to note that the harmonisation of legislation with the EU legal framework and NATO standards is a priority for Ukraine.

First of all, NIS 2 of Directive 2022/2555 should be taken as a basis and a new version of the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" should be adopted, taking into account the key provisions of the Directive. Moreover, the new version should contain mechanisms for risk assessment, timely response to them, reporting on incidents, etc. To ensure that the process is holistic, an interagency working group should also be set up, com-

prising representatives of the National Security and Defence Council, the State Service for Special Communications, the Security Service of Ukraine and other relevant agencies.

The equally important step is to apply for the appropriate partner status in ENISA, which, in turn, will facilitate the participation of Ukrainian experts in ENISA Council meetings and access to timely and relevant information on cyber threats. In the framework of cooperation with NATO, it is worth developing a kind of roadmap for interoperable digital interoperability that will cover both organisational, legal and technical aspects of integration. The creation of a joint body to share experience in responding to cyber threats, such as the NATO Tallinn Project, is also relevant in the current context. Such a move would bring significant positive results and strengthen Ukraine's ability to respond to cyber threats in a timely manner and ensure information sovereignty (Lehominova et al., 2023).

An important development in the framework of cooperation with NATO and compliance with NATO standards was the audit of the DELTA combat system. This is the first time that the system has been certified for information security according to NATO standards.

The benefits of harmonizing Ukrainian legislation with international standards, including a higher level of information sovereignty and national security, strengthening legal instruments to protect critical information systems in line with NATO recommendations and key EU documents, and improving interoperability with allies in the context of the ongoing hybrid war. This will allow for integration into joint cybersecurity and data exchange exercises, as well as improved response to potential threats. A higher level of resilience to potential cyber threats also depends on the legal framework and the consistency of norms between them. Ukraine can improve the protection of its financial systems and energy networks by learning from the experience of its partners (Pleskach et al., 2020).

3.3. The role of information law in ensuring national security and information sovereignty of the state

Information law plays a strategic role due to its innovative nature and integrative functionality in ensuring national security and defence in the digital age. Undoubtedly, the war complicates the digitalisation process, but information law today goes beyond the traditional framework, taking on the responsibility of be-

coming a proactive tool for the state's existence in the digital space. At the same time, the strategic role of information law is directly manifested in the integration and use of protection mechanisms in the digital space (Pravdyuk, 2024).

It is important to note that as part of the work to improve Ukraine's legal system in the area of cybersecurity and introduce defence principles into current legislation, in parallel with international standards, information law is becoming a kind of barrier against external attacks. At the same time, the proposed norms are being actively coordinated with the broader security strategy of the state in order to increase the state's resilience to new hybrid threats (Savchuk, 2024).

This role of information law is accompanied by both risks and opportunities. As for the opportunities, it opens up the possibility of using AI and blockchain technologies, thereby strengthening Ukraine's defence capabilities. However, on the other hand, this will help to identify new risks and weaknesses caused by attacks also using artificial intelligence. That is why it is necessary to update the existing laws in order to not only respond to new risks in a timely manner, but also to be able to anticipate and predict them (Kormych et al., 2024).

Information law is important in the context of international cooperation and harmonization of legislation. This means that by solving problems inside and outside the country, information law becomes a cornerstone of a comprehensive national strategy of information sovereignty (Kormych et al., 2024). In practice, the strategic deployment of information law requires a proactive position. It should go beyond static rules to include dynamic protection mechanisms, such as real-time reporting of cyber incidents, public-private partnerships, and legal incentives for cybersecurity innovation. For Ukraine, this could mean amending existing laws to make resilience testing of critical infrastructure mandatory or creating a legal framework for digital security education for citizens – measures that strengthen the defences of both the state and society (Savchuk, 2024).

It should also be noted that information law has the resource to transform Ukraine's vulnerabilities and strengths. This is manifested in the need to develop a comprehensive national strategy that will present information law as a proactive tool for protecting information sovereignty as such (Babichev & Peliukh, 2024). In this study, it is proposed to address the following aspects of the national strategy aimed at protecting and securing the information space of the state and supporting information sovereignty. In this case, the information space should

be regarded as a critical line of state defense, with the obligatory involvement of international partnership.

Work on strengthening legal norms in the context of the ongoing war and martial law – within this framework, it is proposed to develop protocols for capturing and isolating networks that are compromised or pose a direct threat to Ukraine's sovereignty. In the context of this proposal, it is believed necessary to adopt a relevant legal act that would regulate the protection of critical state data. This data would be stored on Ukraine's internal servers, with copies on servers of allied countries. It is also worth emphasising measures to counter hybrid threats by providing a comprehensive legal interpretation and imposing responsibility for hybrid attacks, treating them as direct military action (The National Security and Defense Council of Ukraine, 2023).

Harmonization of current legislation in line with NATO and EU international standards. In this area, in addition to the proposals outlined in the previous section, it is also proposed to join and create cross-border cyber alliances by concluding agreements with partner countries to exchange data on cyber threats. It is also believed that it is important to adopt global protocols for cybersecurity management based on international standards, adapting them to Ukraine's current needs. This will help build trust and attract foreign investment in technology resilience (Babichev & Peliukh, 2024).

Actively fighting cyberattacks and hybrid threats, including the creation of artificial intelligence systems that will combine private, public and military networks to identify potential threats and eliminate them (Verkhovna Rada of Ukraine, 2023a; 2023b). It is also proposed to engage private firms in combating cyberattacks, with mandatory cooperation with state-authorized institutions.

Such cooperation could include the exchange of compromise indicators and general data on cyber threats, and the creation of a forum for planning tactics to combat cyber threats and analysing the latest cybersecurity trends. This could also facilitate the deployment of blockchain technologies to verify official messages and debunk fakes, based on the 2014 Crimean propaganda textbook. Moreover, such cooperation should include certain security protocols that would guarantee data confidentiality, protection of commercial information of private and public institutions, and compliance with the current legislation on personal information protection.

The following pillars of implementation should be established, with a special agency under the Ministry of Digital Transformation to oversee the improvement of legislation and the implementation of the strategy in joint coordination with the SSU and the relevant NATO body. In parallel, appropriate tax incentives or grants should be offered for the development of advanced cybersecurity tools and mechanisms.

Optimise national cybersecurity structures to improve response to potential threats. An important aspect of optimisation is the introduction of a system of key performance indicators (KPIs) to assess the performance of cybersecurity structures (Pravdyuk, 2024). As for the KPIs themselves, they may include the time taken to respond to an incident, the number of incidents that were resolved, and the level of preparedness of critical infrastructure against cyber threats. This will help to effectively evaluate existing units and future units created as part of the strategy. These proposals for the development of a national strategy aimed at protecting and securing the state's information space and supporting information sovereignty will expand the scope of cooperation and facilitate more active work on these issues.

3. *Conclusion*

Information sovereignty is defined as the ability and right of the state to independently formulate and implement its information policy, manage information resources, existing infrastructure and ensure security in the information space at its own discretion. The ability to protect the population from the results of massive cyberattacks by an external enemy, to be resistant to information warfare, based on the state's ability to manage the information received by the population, for which it is necessary to create appropriate conditions.

The harmonization of Ukraine's strategic directions of security and relevant Ukrainian legislation with international standards is also important, as it can improve information and cybersecurity and help to counter hybrid threats more effectively. The basis of the legislative framework on cybersecurity is the Constitution of Ukraine, the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine", the Criminal Code of Ukraine, the Law of Ukraine "On Information", the Law of Ukraine "On Information Protection in Information and Telecommunications Systems", the Law of Ukraine "On the State Service of

Special Communications and Information Protection of Ukraine", the Decision of the National Security and Defense Council of Ukraine "On the Cybersecurity Strategy of Ukraine", the Action Plan for the Implementation of the Provisions of the Cybersecurity Strategy of Ukraine for 2023-2024, the Resolution of the Cabinet of Ministers of Ukraine "On Some Issues of Response of Cybersecurity Entities to Various Types of Events in Cyberspace", the Convention on Cybercrime, which was ratified by Ukraine in 2005, the Law of Ukraine "On Critical Infrastructure" and the Resolution of the CMU "On Approval of General Requirements for Cybersecurity Protection of Critical Infrastructure".

The legal acts were adopted at different times, it is quite obvious that there are inconsistencies in terminology, overlapping accountability, gaps and contradictions, lack of provisions for conducting information security audits of critical infrastructure, etc. It is also important to understand the problems faced during cyberattacks and what needs to be taken into account when aligning the legal framework.

These challenges include: low or insufficient qualifications of cybersecurity personnel; complex cyberattacks; the need for effective monitoring tools; lack of rapid adaptation to changing threats; lack of financial resources; and problematic communication between relevant departments. An analysis of the peculiarities of cybersecurity regulation in the EU and NATO standards reveals the following advantages of harmonizing Ukrainian legislation with international standards: a high level of information sovereignty and national security; strengthening of legal instruments; improved interoperability with allies; and increased resilience to potential cyber threats.

The study proposes several national strategies aimed at protecting and securing the state's information space and preserving information sovereignty. The following strategies include: work on strengthening legal norms in the context of the ongoing war and martial law; harmonization of current legislation in accordance with NATO and EU international standards; active fight against cyberattacks and hybrid threats, including the creation of artificial intelligence systems that will integrate private, public and military networks; creation of a national cybersecurity system; creation of a national cybersecurity network. These steps will help to improve the situation with information sovereignty in the face of gabyridic threats.

References

Babichev, A. V. & Peliukh, O. I. (2024). Improving cybersecurity mechanisms in Ukraine: The political and administrative aspects. *Business Inform, 9*, 139-147. https://doi.org/10.32983/2222-4459-2024-9-139-147

Chander, A., & Haochen, S. (2023). Introduction: Sovereignty 2.0. In A., Chander, and H. Sun (Eds), *Data sovereignty: From the digital silk road to the return of the state*. New York: Oxford Academic.

Cyber Risk GmbH. (2024). The European cyber resilience act (CRA). (2024). Retrieved from https://www.european-cyber-resilience-act.com

Didkivska, G. & Shevchenko, D. (2024). Basic principles of combating cybercrime: International experience. *Legal Horizons, 19*(4), 19-23. https://doi.org/10.54477/LH.25192353.2023.4.pp.19-23

H-X Technologies. (2024). European Union strengthens cybersecurity measures. Retrieved from https://www.h-x.technology/ua/services/eu-cra-cyber-resilience-act-ua

Khmyrov, I. (2023). Mechanisms of state regulation of information policy in conditions of hybrid threats as a key element of state sovereignty. *Bulletin of the National University of Civil Protection of Ukraine, 2*(21), 150-156. https://doi.org/10.52363/2414-5866-2024-2-17

Khudoliy, A., Sydoruk, T., & Balatska, O. (2024). *Modern challenges: Security and EU: A handbook of the certificate program*. Ostroh: The National University of Ostroh Academy Publishing House.

Kormych, L., Krasnopolska, T. & Zavhorodnia, Yu. (2024). Digital transformation and national security ensuring. *Evropsky Politicky a Pravni Diskurz, 11*(1), 29-37. https://doi.org/10.46340/eppd.2024.11.1.4

Kotsur, V., Hovpun, O., Podhorets, S., Metil, A., & Chasova, T. (2023). State regulation of anti-corruption activities in Ukraine during martial law. *Journal of International Legal Communication, 11*(4), 65-79. https://doi.org/10.32612/uw.27201643.2023.11.4.pp.65-79

Lehominova, S.V., Shchavinskyy, Yu.V., Muzhanova, T.M., Dzyuba, T.M., & Rabchun, D.I. (2023). Legal mechanisms of ensuring information security of Ukraine in the conditions of hybrid war. *Telecommunications and Information Technologies, 1*(78), 101-110. https://doi.org/10.31673/2412-4338.2023.0101111

Neustroiev, Y. (2021). The role of innovation in ensuring economic security. *Agrosvit, 7-8*, 103-108. https://doi.org/10.32702/2306-6792.2021.7-8.103

North Atlantic Treaty Organization. (2024). Cyber defence. Retrieved from https://www.nato.int/cps/en/natohq/topics_78170.htm

Pleskach, M., Pleskach, V., Semenchenko, A., Myalkovsky, D., & Stanislavsky T. (2020). Standardization in the field of cybersecurity and cyber protection in Ukraine. *Information & Security: An International Journal,45,* 57-76. https://doi.org/10.11610/isij.4504

Pravdyuk, A.L. (2024.). Information sovereignty in the context of information security. *Scientific Innovations and Advanced Technologies, 11*(39), 639-651. https://doi.org/10.52058/2786-5274-2024-11(39)-639-651

Savchuk, S. (2024). Challenges and prospects for the formation of state policy in the field of cybersecurity and combating cybercrime. *Public Policy and Accounting, 1*(9), 30-38. https://doi.org/10.26642/ppa-2024-1(9)-30-38

Solodka, O.M. (2024). Information sovereignty of the state: On the issue of ensurence. *Legal Scientific Electronic Journal, 9*, 267-270. https://doi.org/10.32782/2524-0374/2024-9/62

Sopilko, I. (2024). Strengthening cybersecurity in Ukraine: Legal frameworks and technical strategies for ensuring cyberspace integrity. *Legal Horizons, 21*(2), 69-80. https://doi.org/10.54477/LH.25192353.2024.2.pp.69-80

The National Security and Defense Council of Ukraine. (2023). Harmonization of cyber security systems of critical infrastructure with EU standards was discussed at the meeting of the National Cyber Security Cluster in Warsaw. Retrieved from https://www.rnbo.gov.ua/en/Diialnist/6237.html

Vasylkivska, I.P., & Bondarenko, Y.I. (2023). Information and cyber security in the light of hybrid threats. *Visegrad Journal on Human Rights*, 38-42.

Verkhovna Rada of Ukraine. (1992). On information. Retrieved from https://zakon.rada.gov.ua/laws/show/2657-12#Text

Verkhovna Rada of Ukraine. (1994). On information protection in information and communication systems. Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-вр#Text

Verkhovna Rada of Ukraine. (1996). Constitution of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

Verkhovna Rada of Ukraine. (2001). Criminal Code of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text

Verkhovna Rada of Ukraine. (2005a). On the ratification of the Convention on cybercrime. Retrieved from https://zakon.rada.gov.ua/laws/show/2824-15#Text

Verkhovna Rada of Ukraine. (2005b). On the resolution of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the cybersecurity strategy of Ukraine". Retrieved from https://www.president.gov.ua/documents/4472021-40013

Verkhovna Rada of Ukraine. (2006). On the State Service for Special Communications and Information Protection of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/3475-15#Text

Verkhovna Rada of Ukraine. (2017). On the basic principles of ensuring cybersecurity in Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text

Verkhovna Rada of Ukraine. (2019). On approval of general requirements for cybersecurity of critical infrastructure facilities. Retrieved from https://zakon.rada.gov.ua/laws/show/518-2019-п#Text

Verkhovna Rada of Ukraine. (2023a). Some issues of response by cybersecurity entities to various types of events in cyberspace. Retrieved from https://zakon.rada.gov.ua/laws/show/299-2023-п#Text

Verkhovna Rada of Ukraine. (2023b). On approval of the action plan for 2023-2024 on the implementation of the cybersecurity strategy of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/1163-2023-p#Text

Verkhovna Rada of Ukraine. (2023c). On critical infrastructure. Retrieved from https://zakon.rada.gov.ua/laws/show/1882-20#Text

Vorotynskyy, V. (2024). The impact of hybrid warfare on the formation of state information sovereignty of Ukraine. *Legal Scientific Electronic Journal, 9*, 267-270. https://doi.org/10.33663/1563-3349-2024-95-266

Breastplate of the Ukrainian Ministry of Defense
Author: Олекса Руденко 1990. Public Domain
Wikimedia Commons

Special Dossier October 2025
Ukraine Military and Wartime Law

Articoli / Articles